ISSN 2084-9079

RAPORT 2012

CERT Polska

Analiza incydentów naruszających bezpieczeństwo teleinformatyczne

Zespół CERT Polska działa w ramach Naukowej i Akademickiej Sieci Komputerowej

CERT POLSKA NASK

Raport CERT Polska

Wydawca: NASK

Adres: ul. Wąwozowa 18, 02-796 Warszawa, | tel. (22) 38 08 200, e-mail: cert@cert.pl

Opracowanie i redakcja: CERT Polska

Projekt graficzny, skład i łamanie: Piu Professional

Spis treści

1 Wprowadzenie

CERT Polska od 1996 roku przygotowuje i udostępnia roczne statystyki dotyczące incydentów bezpieczeństwa teleinformatycznego w polskich zasobach internetowych, które zostały zgłoszone do zespołu. Niniejszy raport ma na celu nakreślenie obrazu bezpieczeństwa polskiego Internetu oraz przedstawienie aktualnych trendów w tej dziedzinie.

Raport składa się z pięciu głównych części. W rozdziałach 2 i 3 szczegółowo zaprezentowane zostały statystyki oraz analiza zdarzeń koordynowanych i obsługiwanych przez CERT Polska.

Rozdział 2 zawiera informacje na temat zagrożeń w polskich sieciach, przekazane zespołowi CERT Polska przez różne podmioty związane z monitorowaniem i reagowaniem na zagrożenia oraz zebrane przez własne systemy. Ponieważ uwzględniają one prawie wszystkich polskich operatorów, dają bardzo szeroki obraz tego, co naprawdę dzieje się w polskich zasobach internetowych.

Rozdział 3 skupia się na działalności operacyjnej CERT Polska. Dane w nim przedstawione pochodzą z systemu obsługi incydentów i przedstawiają zdarzenia, w których CERT Polska interweniował.

Ze wszystkich zjawisk dotyczących bezpieczeństwa w 2012 roku wybraliśmy siedem, w których analizę byliśmy zaangażowani i które uznaliśmy za warte bliższego przyjrzenia się. Zostały one opisane w rozdziale 4.

Rozdział 5 to opis niektórych inicjatyw w ramach krajowej i międzynarodowej aktywności CERT Polska w ubiegłym roku.

Specjalnie wydzieloną częścią opracowania jest raport z systemu wczesnego ostrzegania ARAKIS, zawierający między innymi statystyki dotyczące alarmów generowanych przez system oraz opisy interesujących przypadków dokonanych w nim obserwacji.

Warto zaznaczyć, że porównywanie tegorocznego raportu z opracowaniami z lat ubiegłych, mimo zachowania tej samej kategoryzacji zdarzeń, mija się z celem. Ma na to wpływ kilka czynników opisanych szczegółowo w treści raportu. Przede wszystkim duży wpływ na statystyki mają zmiany w ilości i rodzaju danych otrzymywanych przez CERT Polska od podmiotów zewnętrznych.

W tym roku, dla przedstawienia rozszerzonego obrazu zdarzeń bezpieczeństwa u operatorów w różnych kategoriach zagrożeń, oprócz bezwzględnej liczby zdarzeń bezpieczeństwa w sieciach operatora, wzięliśmy pod uwagę także wielkość tych sieci.

1.1 Najważniejsze obserwacje podsumowujące raport

- W 2012 roku CERT Polska odnotował ponad 10,5 mln automatycznych zgłoszeń dotyczących naruszeń bezpieczeństwa, przede wszystkim przypadków źródeł spamu oraz botów.

- Po raz pierwszy od 2005 roku wzrosła liczba incydentów obsłużonych przez CERT Polska ręcznie, a więc tych najpoważniejszych. W 2012 roku było ich 1 082, czyli o blisko 80 % więcej niż przed rokiem – głównie za sprawą złośliwego oprogramowania i phishingu.

- Polska wypada dobrze na tle innych krajów pod względem liczby utrzymywanych w naszym kraju stron związanych z phishingiem i złośliwym oprogramowaniem – w statystykach znajdujemy się poza pierwszą dziesiątką. Niestety, znacznie gorzej jest w przypadku problemów związanych z komputerami użytkowników indywidualnych, a więc liczby botów, skanowań i wysyłanego spamu. Przyczyniają się do tego przede wszystkim sieci operatorów komórkowych, oferujących mobilny dostęp do Internetu, a także Netia – jeden z największych operatorów telekomunikacyjnych.

- Najwięcej zgłoszeń botów, a więc zainfekowanych komputerów, sterowanych centralnie przez specjalne kontrolery, dotyczyło trzech rodzajów złośliwego oprogramowania: Viruta, DNSChangera oraz różnych odmian ZeuSa. Łącznie każdego dnia obserwowaliśmy średnio ok. 8 000 botów zarażonych tymi wirusami.

- Obserwujemy systematyczny wzrost liczby incydentów związanych z phishingiem – zarówno w tradycyjnej formie, polegającej na tworzeniu stron podszywających się pod banki, sklepy internetowe itp., jak i związanego ze złośliwym oprogramowaniem potrafiącym modyfikować zawartość stron bankowych odwiedzanych przez użytkownika.

- Najczęściej atakowaną usługą w przypadku skanowań jest niezmiennie SMB w Microsoft Windows (445/TCP). Robaki propagujące się z wykorzystaniem tej usługi, takie jak Sasser czy Conficker wciąż „mają się dobrze”, choć powstały 5 i więcej lat temu!

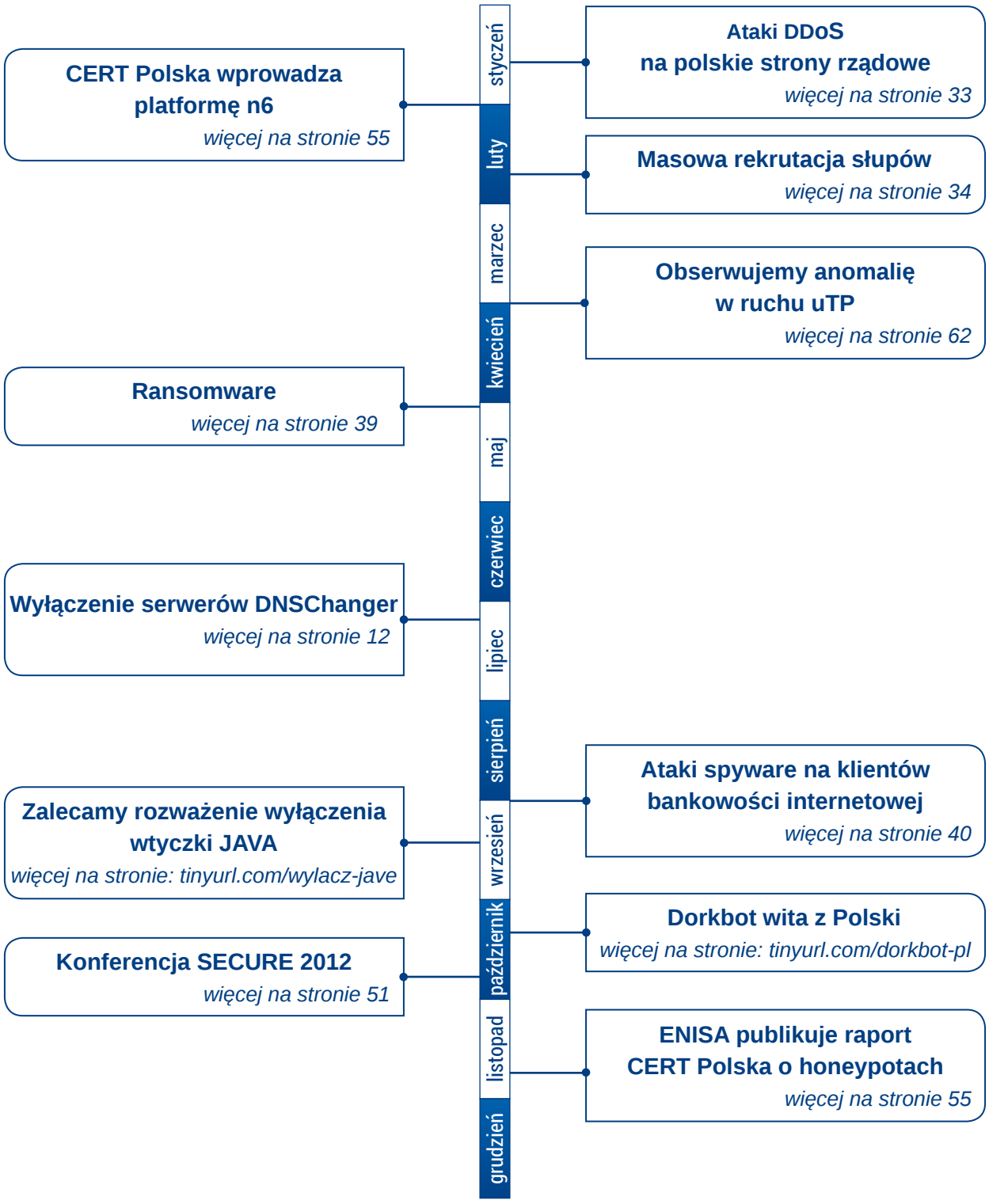
- Nowością wśród często atakowanych usług jest Zdalny Pulpit w systemach MS Windows (3389/TCP) . Ataki polegają przede wszystkim na próbie odgadnięcia haseł do tej usługi, co pozwala na przejęcie kontroli nad pulpitem. Za dużą część takich ataków odpowiada robak Morto.

- Znacząco, bo aż o 56 %, powiększyła się liczba serwerów DNS w polskich sieciach, które skonfigurowane są w nieprawidłowy sposób, narażając na niebezpieczeństwo wszystkich użytkowników sieci. Powodem jest głównie brak świadomości istnienia problemu u ich administratorów.

- W zgłoszeniach trafiających do ręcznego systemu obsługi wzrasta przewaga tych pochodzących z zagranicznych podmiotów komercyjnych nad zgłoszeniami od osób prywatnych z Polski. Dotyczy to przede wszystkim incydentów związanych ze spamem i phishingiem.

1.2 Zestawienie wydarzeń w czasie

Poniższy rysunek przedstawia chronologicznie uporządkowanie istotnych zdarzeń z obszaru działalności CERT Polska, które zostały opisane w raporcie.



1.3 Informacje o zespole CERT Polska

Zespół CERT Polska działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) - instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty (z ang. Computer Emergency Response Team). Aktywnie operując od 1996 roku w środowisku zespołów reagujących, stał się rozpoznawalnym i doświadczonym podmiotem w dziedzinie bezpieczeństwa komputerowego. Od początku istnienia rdzeniem działalności zespołu jest obsługa incydentów bezpieczeństwa i współpraca z podobnymi jednostkami na całym świecie, zarówno w działalności operacyjnej, jak i badawczo-wdrożeniowej. Od 1998 roku CERT Polska jest członkiem międzynarodowego forum zrzeszającego zespoły reagujące - FIRST, a od roku 2000 należy do grupy roboczej europejskich zespołów reagujących - TERENA TF-CSIRT i działającej przy niej organizacji Trusted Introducer. W 2005 roku z inicjatywy CERT Polska powstało forum polskich zespołów abuse - Abuse FORUM, natomiast w 2010 r. CERT Polska dołączył do Anti-Phishing Working Group, stowarzyszenia gromadzącego firmy i instytucje aktywnie walczące z przestępczością w sieci.

Do głównych zadań zespołu CERT Polska należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci;
- aktywne reagowanie w przypadku wystąpienia bezpośrednich zagrożeń dla użytkowników;
- współpraca z innymi zespołami CERT w Polsce i na świecie;
- udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego;
- działalność badawcza z zakresu metod wykrywania incydentów bezpieczeństwa, analizy złośliwego oprogramowania, systemów wymiany informacji o zagrożeniach;
- rozwijanie własnych narzędzi do wykrywania, monitorowania, analizy i korelacji zagrożeń;
- regularne publikowanie Raportu CERT Polska o bezpieczeństwie polskich zasobów Internetu;
- działania informacyjno-edukacyjne, zmierzające do wzrostu świadomości w zakresie bezpieczeństwa teleinformatycznego, w tym:
  - publikowanie informacji o bezpieczeństwie na blogu **http://www.cert.pl/** oraz w serwisach społecznościowych Facebook i Twitter;
  - organizacja cyklicznej konferencji SECURE;
- niezależne analizy i testy rozwiązań z dziedziny bezpieczeństwa teleinformatycznego.

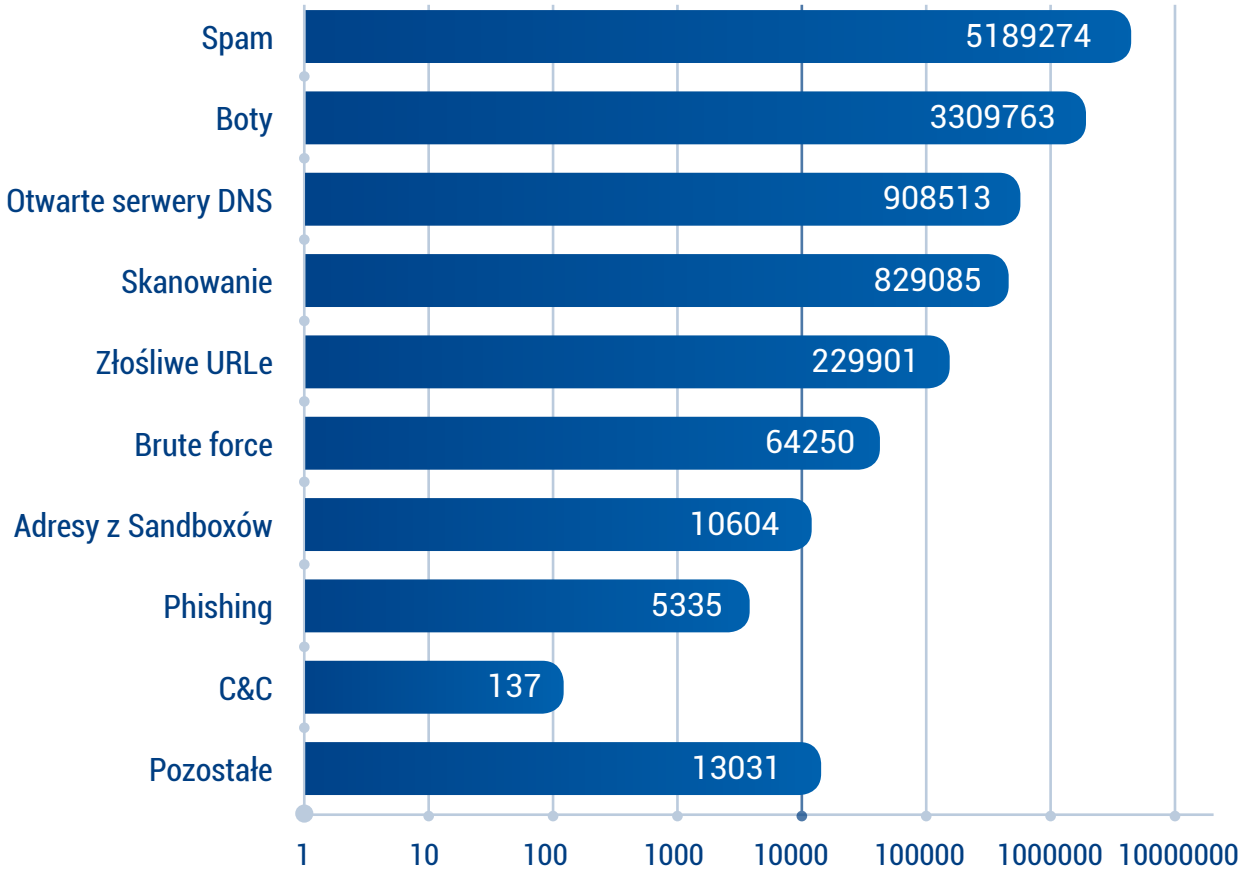
2 Statystyka zgłoszeń koordynowanych przez CERT Polska

W tej części raportu prezentujemy opracowane przez CERT Polska statystyki otrzymanych przez zespół zgłoszeń, zarówno ze źródeł zewnętrznych jak i z wewnętrznych, własnych systemów.

2.1 Ilość informacji we wszystkich kategoriach

W roku 2012 otrzymaliśmy 10 559 893 zgłoszenia pochodzące z systemów autonomicznych - prawie dokładnie o połowę mniej niż w roku 2011. Jedną z przyczyn mniejszej liczby zgłoszeń są zmiany w liczbie źródeł oraz rodzaju danych z nich pochodzących. Dobrym przykładem tego jest zakończenie monitorowania botnetu Conficker po definitywnym usunięciu infrastruktury nim zarządzającej. Inną przyczyną jest zmiana sposobu zliczania niektórych zgłoszeń, pośrednio wynikająca także z faktu zmiany źródeł.

Z powodów opisanych powyżej porównywanie liczb bezwzględnych pomiędzy kolejnymi latami nie jest miarodajne ani dla łącznej liczby zgłoszeń, ani dla poszczególnych kategorii. Porównanie poszczególnych kategorii między sobą przedstawione na Rysunku 1 może służyć jedynie jako obraz ilości informacji, które przetwarzamy, a nie skali poszczególnych problemów. Warto podkreślić, że bardzo wiele zależy od tego, jak w różnym stopniu skuteczne są metody wykrywania zdarzeń, stosowane przez podmioty wymieniające z nami dane, a także od bieżących obszarów zainteresowania środowiska.



Rysunek 1. Liczba zgłoszeń automatycznych w poszczególnych kategoriach

2.2 Spam

Incydenty opisane w tym punkcie dotyczą maszyn w polskich sieciach, będących źródłem niezamówionej korespondencji. W ogromnej większości są to komputery zarażone złośliwym oprogramowaniem, a więc boty, które wykorzystywano do masowej wysyłki spamu bez wiedzy ich właścicieli.

W 2012 roku otrzymaliśmy 5 189 274 zgłoszeń dotyczących rozsyłania spamu z polskich adresów IP, o 10,9% więcej niż w 2011 roku. Dotyczyły one 1 648 009 adresów IP (wzrost o 31,5% w stosunku do roku 2011).

Jedną z przyczyn dużego wzrostu liczby adresów IP raportowanych jako wysyłające spam jest nasilenie trendu, który sygnalizowaliśmy już w ubiegłych latach: coraz więcej przypadków dotyczy sieci mobilnych, które adresy IP przydzielają w sposób dynamiczny i na krótki czas. W rezultacie użytkownik zainfekowanego laptopa korzystający z mobilnego dostępu do Internetu będzie „widziany" wielokrotnie pod różnymi adresami IP, nawet w ciągu jednego dnia. W tym roku skala problemu jest już alarmująca – sieci mobilnych dotyczy aż 36,7% zgłoszeń. To blisko 2 miliony w liczbach bezwzględnych! Problem jest jeszcze poważniejszy, gdy przyjrzymy się „zanieczyszczeniu" poszczególnych sieci, to znaczy udziałowi adresów IP zgłoszonych jako rozsyłające spam w ogólnej puli należącej do danego operatora. W przypadku P4 (operatora sieci Play) sięga on aż 40,6%, co oznacza, że dwa na każde pięć adresów były wykorzystywane do rozsyłania spamu. W przypadku innych operatorów mobilnych jest nieco lepiej, jednak 13,9-16,0% to nadal sporo. Konsekwencją może być między innymi umieszczenie sieci tych operatorów na czarnych listach.

Pierwsze miejsce w bezwzględnej liczbie zgłoszeń po raz kolejny przypada Netii (blisko 972 tys., 18,7%). Netia ma także bardzo wysoki odsetek adresów rozsyłających spam w swojej sieci (20,1%), choć należy przyznać, że względem 2011 roku zarówno liczba zgłoszeń, jak i liczba unikalnych adresów IP wysyłających spam w Netii znacząco się zmniejszyły.

Nie najlepiej wypadają też największe sieci kablowe: Multimedia Polska i Vectra. Znalazły się one w czołówce tabeli nie tylko ze względu na liczbę zgłoszeń (odpowiednio 8,2% i 5,3% ogółu), która mogłaby wynikać z rozmiarów sieci, ale także ze względu na duży odsetek IP zgłaszanych jako źródła spamu (odpowiednio 14,5% oraz 9,8%). W zestawieniu nie została ujęta sieć UPC, ponieważ wiele źródeł raportuje jej adresy jako należące do zagranicznej centrali firmy.

Po raz kolejny pozytywnym przykładem jest sieć Telekomunikacji Polskiej (obecnie pod marką Orange Polska). Liczba zgłoszeń dotyczących tej sieci spadła o blisko 1/3 w stosunku do 2011 roku do poziomu 504 tys., co spowodowało poprawę pozycji TP o dwa miejsca (z drugiego na czwarte). Zgłoszenia dotyczyły jednak tylko 43 tys. unikalnych IP, co stanowi zaledwie 0,6% całej sieci! Tak znakomity wynik TP zawdzięcza stosowaniu polityki domyślnego blokowania portu 25 TCP, co - jak się okazuje - sprawdza się doskonale.

Blokowanie portu 25 TCP nie usuwa niestety źródła problemu (zainfekowanych maszyn), co dobrze widać w rozdziałach 4.5 i 4.2, jest jednak korzystne z kilku powodów: po pierwsze zmniejsza uciążliwość spamu dla innych użytkowników Internetu, a po drugie uderza w model biznesowy stosowany przez przestępców. Warto postawić pytanie, kiedy śladem TP pójdą inni dostawcy w Polsce.

	Zmiana	Numer AS	Nazwa operatora	Liczba zgłoszeń	Zmiana	Udział	Liczba unikalnych IP	Zmiana	Udział IP
1	-	12741	Netia SA	971 682	▼ 480 536	18,7%	348 102	▼ 43 303	20,1%
2	▲ 2	43447	PTK Centertel Sp. z o.o.	829 094	469 016	16,0%	317 257	122 938	14,0%
3	▲ 4	39603	P4 Sp. z o.o.	507 940	325 340	9,8%	326 816	179 262	40,6%
4	▼ 2	5617	TP S.A.	503 714	▼ 293 561	9,7%	43 102	▼ 64 375	0,6%
5	▼ 2	21021	Multimedia Polska S.A.	425 417	▼ 43 515	8,2%	88 102	17 837	14,5%
6	▲ 3	12912	Polska Telefonia Cyfrowa S.A.	325 420	228 137	6,3%	21 6897	137 619	15,1%
7	▼ 2	29314	VECTRA	276 020	▼ 77 978	5,3%	43 213	23 549	9,9%
8	▼ 2	8374	Polkomtel S.A.	242 910	▼ 22 837	4,7%	21 1702	2 2751	16,0%
9	▼ 1	20960	TK Telekom	106 478	▼ 21 815	2,1%	4 287	▼ 1 171	1,6%
10	N	6714	ATOM SA	55 036	BD	1,1%	14 686	BD	3,4%

Tabela 1. Najczęściej raportowane sieci (według numerów AS)

W poniższej tabeli uwzględniono 13 największych polskich systemów autonomicznych (o puli ponad 250 tysięcy adresów) według odsetku adresów IP raportowanych jako wysyłające spam (pominięto należący do UPC AS12476):

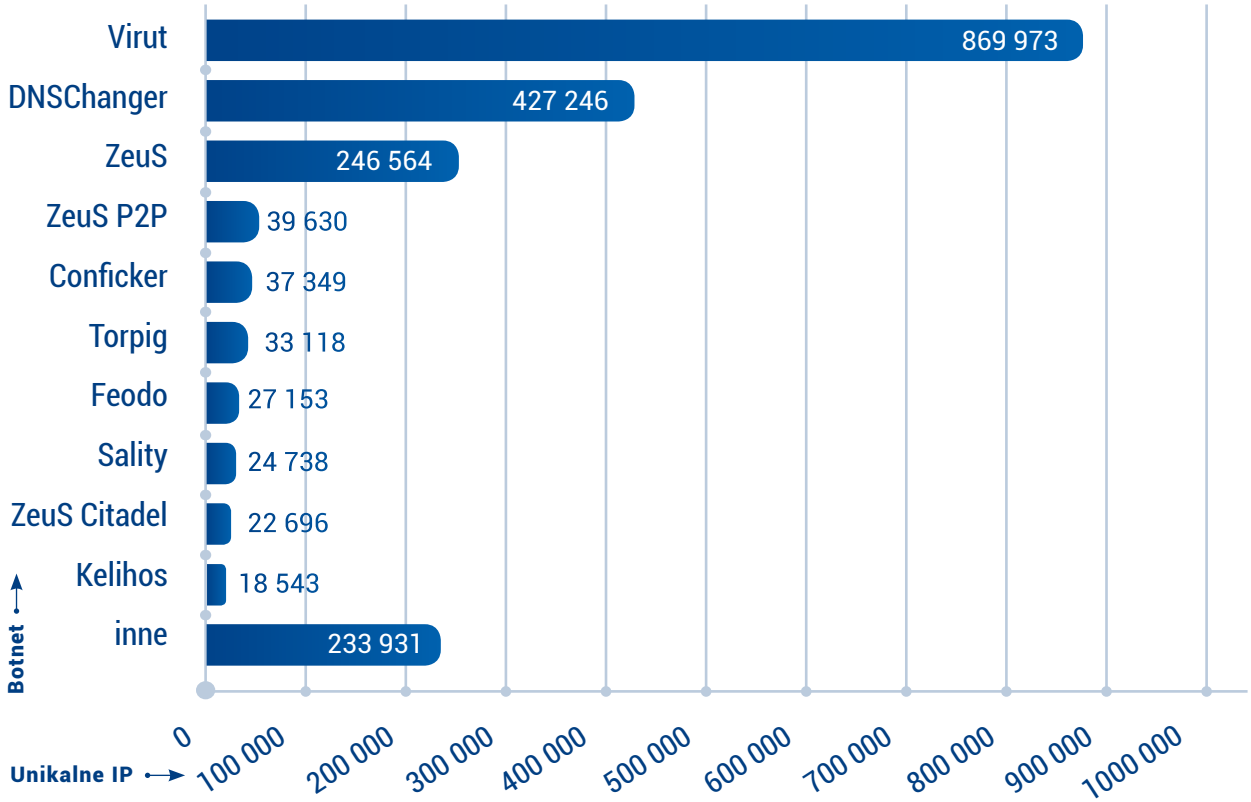
	Numer AS	Nazwa operatora	Unikalne IP	Odsetek
1	39603	P4 Sp. z o.o.	326 816	40,605%
2	12741	Netia SA	348 102	20,145%
3	8374	Polkomtel S.A.	211 702	16,002%
4	12912	Polska Telefonia Cyfrowa S.A.	216 897	15,130%
5	21021	Multimedia Polska S.A.	88 102	14,460%
6	43447	PTK Centertel Sp. z o.o.	317 257	13,954%
7	29314	VECTRA	43 213	9,854%
8	6 714	ATOM SA	14 686	3,424%
9	20960	TK Telekom	4 287	1,612%
10	5617	TP S.A.	43 102	0,623%
11	43939	Internetia Sp.z o.o.	1 382	0,336%
12	15857	Dialog S.A.	1 021	0,230%
13	8308	NASK Commercial	729	0,229%

Tabela 2. Największe polskie numery AS (ponad 250 000 adresów) według odsetku adresów IP raportowanych jako wysyłające spam

2.3 Boty w polskich sieciach

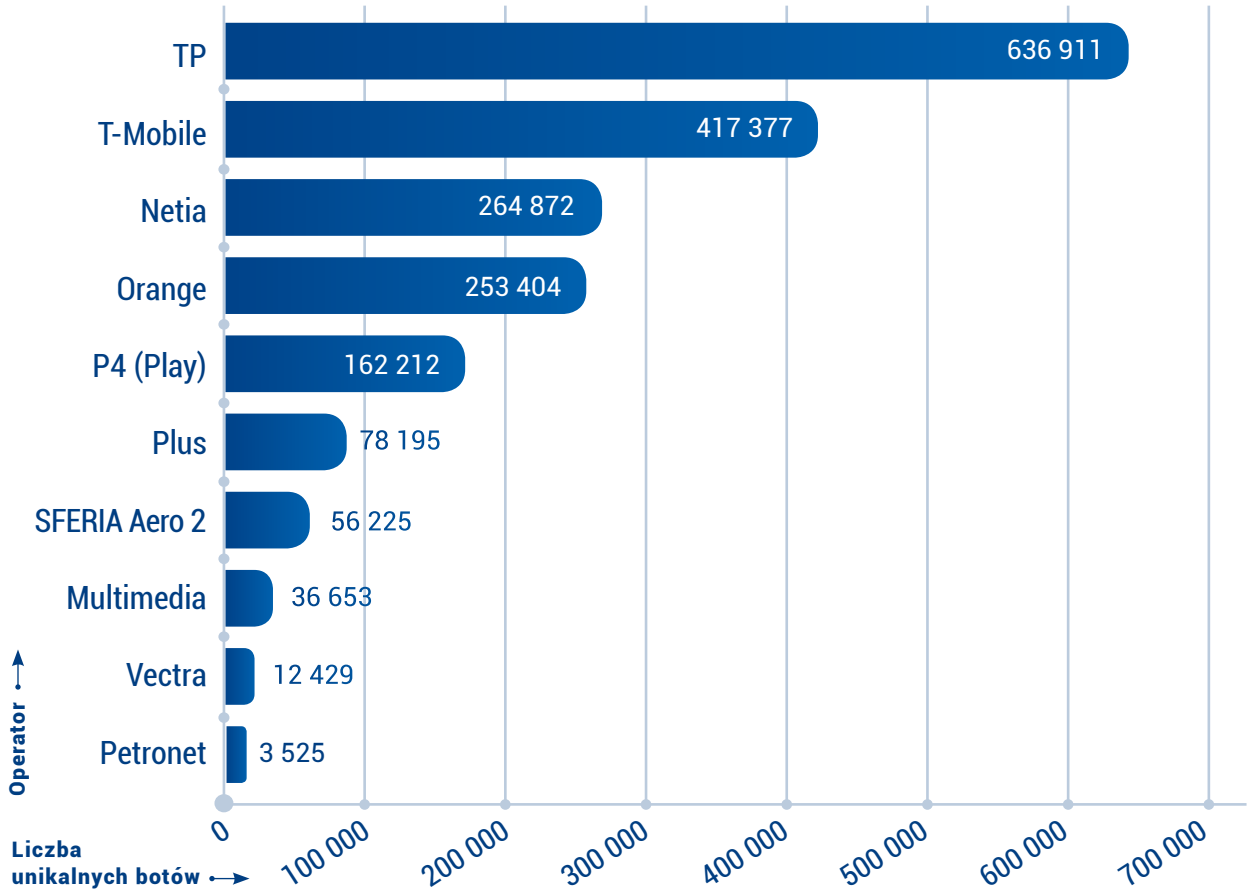
Statystyki te uwzględniają tzw. boty, czyli komputery będące członkami botnetów, znajdujące się w polskich sieciach, a nieuwzględnione w innych kategoriach. Zazwyczaj botnety używane są do wysyłania spamu, wykradania danych, ataków DDoS, lub jako dodatkowa warstwa anonimizacji.

W minionym roku otrzymaliśmy 3 309 763 zgłoszeń raportujących o 1 980 941 unikalnych botach w polskich sieciach. Najwięcej raportów dotyczyło botnetu Virut, przeciw któremu na początku 2013 roku NASK podjął działania przejmując 38 domen związanych z jego działalnością. W całym roku 2012 zidentyfikowanych zostało 869 973 unikalnych adresów IP, które posiadały komputery zarażone tym złośliwym oprogramowaniem. Średnio dziennie informowano nas o 3 931 unikalnych botach podłączonych do tego botnetu. Na drugim miejscu uplasował się DNSChanger – złośliwe oprogramowanie, które podmienia na zainfekowanym komputerze adresy serwerów DNS (więcej: **http://www.cert.pl/news/4936**). Serwery DNS, na które malware przekierowywał, zostały przejęte przez FBI i z dniem 9 lipca 2012 roku wyłączone. Od tego momentu nie otrzymaliśmy żadnego zgłoszenia dotyczącego polskiego IP należącego do tego botnetu. W okresie od stycznia do czerwca zgłoszono nam 427 246 unikalnych adresów IP komputerów zarażonych DNSChanger. Na trzecim i czwartym miejscu znajdują się dwie odmiany groźnego trojana bankowego: ZeuS (246 564 unikalne adresy IP w roku) oraz ZeuS P2P (39 630 unikalne adresy IP w roku). Do tej rodziny należy także plasujący się na dziewiątym miejscu Citadel (22 696 unikalne adresy IP w roku). Conficker, który w zeszłym roku był pierwszy z liczbą ponad 2 mln botów, tym razem znalazł się na piątym miejscu z liczbą zaledwie 37 349 botów. Wynika to z faktu, że botnet został porzucony (pozostały jedynie niewyczyszczone komputery) i w roku 2012 Conficker nie był już masowo monitorowany. Ranking najpopularniejszych botnetów w polskich sieciach przedstawiony jest na rysunku poniżej.



Rysunek 2. Ranking najpopularniejszych botnetów w polskich sieciach

W polskich sieciach najwięcej botów zauważyliśmy w sieci TP (AS5617). Była to liczba 636 911 unikalnych IP w roku. Jest to dużo mniejsza liczba niż przed rokiem (prawie 2,5 mln), co prawdopodobnie wynika z braku zgłoszeń odnośnie robaka Conficker. Na drugim miejscu znalazła się sieć T-Mobile (AS12912) z liczbą 417 377 unikalnych IP w roku (w zeszłym roku sieć ta plasowała się na 6 miejscu). Na trzecim (spadek o jedno oczko) jest Netia (AS12741) z liczbą 264 872 unikalnych IP. Ranking bezwzględny przedstawiający sieci o największej liczbie zainfekowanych unikalnych adresów IP przedstawiono poniżej.



Rysunek 3. Ranking bezwzględny przedstawiający sieci o największej liczbie zainfekowanych unikalnych adresów IP

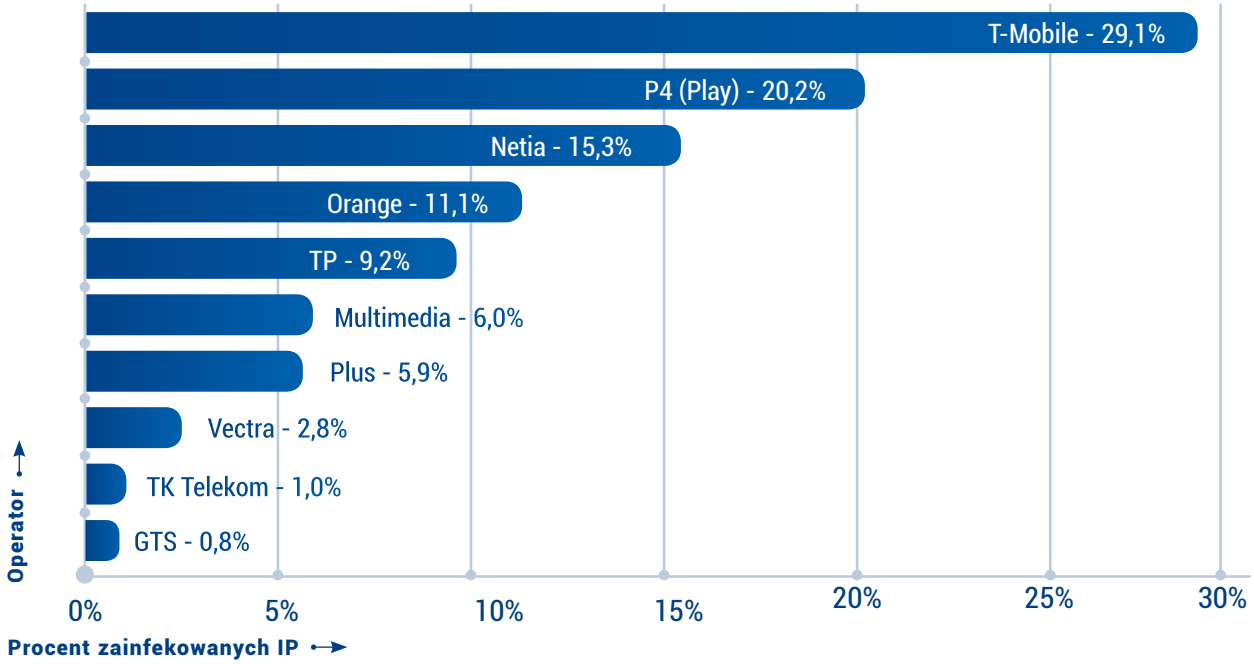
Ogólnie w stosunku do roku 2011 liczba unikalnych IP zaraportowanych do nas znacząco się zmniejszyła. Jest to spowodowane wspomnianym wcześniej zaprzestaniem raportowania informacji o robaku Conficker. Podobnie jak w roku ubiegłym, zaobserwować można w rankingu wysokie pozycje operatorów mobilnych: T-Mobile, Orange, Play i Plus. Dodatkowo, po raz pierwszy w zestawieniu pojawił się operator bezpłatnego dostępu do Internetu Aero 2 (AS15855). Ponadto nie ulega wątpliwości, że najwięcej zainfekowanych komputerów znajduje się w sieciach dużych operatorów, którzy dostarczają Internet odbiorcom indywidualnym: TP, Netia, Multimedia. Ze statystyk Top 10 wypadła sieć Dialog (AS15857) oraz GTS (AS6714), a pojawiła się Petrotel (AS29007).

Wielkość systemu autonomicznego w przypadku powyższego rankingu bezwzględnego wpływa znacząco na pozycję dostawcy – im więcej adresów IP w sieci, tym większa liczba unikalnych botów. Dlatego dodaliśmy jeszcze jedną statystykę uwzględniającą wielkość sieci. Została wprowadzona liczba

określająca procentową wartość liczby unikalnych botów w stosunku do liczby adresów IP należących do danego AS. Liczba adresów IP należących do danego systemu autonomicznego została obliczona z danych znajdujących się w bazie RIPE. W tym rankingu przoduje SFERIA Aero 2 (AS15855), w której liczba unikalnych botów stanowiła aż 83% wszystkich adresów IP. W pierwszej dziesiątce znalazło się aż pięć niewielkich sieci, które składają się z mniej niż 5 000 adresów IP. Wobec tego uznaliśmy, że w statystykach uwzględnimy tylko sieci, które posiadają więcej niż 250 000 adresów IP. Ranking względny przedstawiono w Tabeli 3.

Pozycja	Procent zainfekowanych IP	Liczba unikalnych botów	Numer AS	Nazwa operatora	Pozycja w rankingu bezwzględnym
1	29,1	417 377	12912	T-Mobile	2
2	20,2	162 212	39603	P4 (Play)	5
3	15,3	264 872	12741	Netia	3
4	11,1	253 404	43447	Orange	4
5	9,2	636 911	5617	TP	1
6	6,0	36 653	21021	Multimedia	8
7	5,9	78 195	8374	Plus	6
8	2,8	12 429	29314	Vectra	9
9	1,0	2 535	20960	TK Telekom	15
10	0,8	3 421	6714	GTS	11

Tabela 3. Ranking operatorów wg procentowej wartości liczby botów w stosunku do wielkości AS



Rysunek 4. Ranking operatorów wg procentowej wartości liczby botów w stosunku do wielkości AS

W tak przefiltrowanym rankingu na pierwszym miejscu znajduje się sieć T-Mobile, w której 29% wszystkich adresów przynajmniej raz zostało zgłoszonych jako adresy botów. W ogóle na szczególną uwagę zasługuje fakt wysokich pozycji w obu rankingach operatorów mobilnych. Natomiast znajdująca się na pierwszym miejscu w rankingu bezwzględnym sieć TP tutaj uplasowała się w połowie stawki.

2.4 Otwarte serwery DNS

W zestawieniu tym znajdują się serwery DNS, które, zazwyczaj w wyniku błędnej konfiguracji lub polityki firewalla, umożliwiają rekursywne odpytywanie z dowolnego miejsca w sieci. Taka konfiguracja daje między innymi możliwość wykorzystania ich w atakach DDoS przez zwiększenie wolumenu ruchu w wyniku odpytywania serwerów DNS ze sfałszowanym adresem źródłowym. Problem ten nie zmniejsza się, ponieważ niewielu administratorów zdaje sobie sprawę z tego, że taka konfiguracja może stwarzać problemy, a jeszcze mniej z tego, że w ogóle z taką konfiguracją mają do czynienia. Wydaje się, że rolę informacyjną mogliby pełnić dostawcy internetowi, do których trafiają informacje o nieprawidłowo skonfigurowanych serwerach w ich sieciach.

W 2012 r. otrzymaliśmy 908 513 informacji o 220 666 unikalnych adresach IP, na których znajdowały się opisane wyżej serwery. Liczba unikalnych otwartych serwerów DNS jest wyższa o ponad 37% od zeszłorocznej. To wskazuje na rosnącą skalę tego typu problemu w Polsce. Ranking dziesięciu polskich systemów autonomicznych, w których było umieszczonych najwięcej otwartych serwerów DNS, znajduje się w Tabeli 4. Jest to ranking bezwzględny, który nie bierze pod uwagę wielkości systemu autonomicznego (liczby adresów IP należących do AS).

Pozycja	Zmiana	Liczba unikalnych IP	Udział procentowy	Numer AS	Operator
1	0	82 148	37,2%	5617	TP/Orange
2	▲ 1	36 354	16,5%	43447	Orange
3	▼ 1	18 872	8,6%	12741	Netia
4	▲ 1	7 299	3,3%	6714	ATOM/GTS
5	▼ 1	7 006	3,2%	20960	TK Telekom
6	▲ 1	3 907	1,8%	21021	Multimedia
7	nowość	3 636	1,6%	13110	INEA
8	0	3 062	1,4%	29314	VECTRA
9	▲ 1	3 048	1,4%	13000	Leon
10	▼ 1	2 750	1,2%	29665	Speed-Soft

Tabela 4. Ranking dziesięciu polskich systemów autonomicznych, w których było umieszczonych najwięcej otwartych serwerów DNS

Uwzględniwszy wielkość AS i obliczając liczbę otwartych serwerów na każde 10 adresów IP należących do danego AS otrzymujemy zupełnie inny ranking, gdzie ratio to liczba otwartych serwerów na każde 10 adresów IP należących do AS. Wytłuszczono AS-y, które znalazły się w obu rankingach. Dane o wielkości poszczególnych systemów autonomicznych pobrano z bazy RIPE (stan na 30.01.2013).

Poz.	Ratio	Liczba unikalnych IP	Numer AS	Operator	Pozycja w rankingu bezwzględnym
1	6.89	512	198098	ARTKOM	44
2	5.37	512	29665	Speed-Soft	10
3	4.10	512	47275	Torjon	77
4	3.81	512	47884	JPK	81
5	3.25	1 024	56783	ConnectIT	48
6	3.06	1 024	43607	STREFA	51
7	2.16	1 024	51648	GIGA-AS	69
8	2.00	768	197764	ADWA-NET	95
9	2.00	2 048	16110	Podkarpacki.net	42
10	1.94	2 560	50767	RADIONET-AS ELEKTRO-SYSTEM	30
54	**0.52**	**58 112**	**13000**	**Leon**	**9**
99	**0.26**	**265 984**	**20960**	**TK Telekom**	**5**
111	**0.21**	**168 704**	**13110**	**INEA**	**7**
127	**0.17**	**429 440**	**6714**	**ATOM/GTS**	**4**
130	**0.16**	**2 273 36**	**43447**	**Orange**	**2**
172	**0.12**	**6 916 160**	**5617**	**TP/Orange**	**1**
195	**0.11**	**1 728 000**	**12741**	**Netia**	**3**
291	**0.07**	**438 528**	**29314**	**VECTRA**	**8**
308	**0.06**	**609 280**	**21021**	**Multimedia**	**6**

Tabela 5. Ranking dziesięciu polskich systemów autonomicznych, w których umieszczonych było najwięcej otwartych serwerów DNS (po uwzględnieniu wielkości systemu autonomicznego)

2.5 Skanowanie

Kategoria skanowanie opisuje przypadki wykrytych prób nieautoryzowanych połączeń. Mogą one świadczyć o infekcji komputera, z którego zostało zainicjowane połączenie (np. autopropagacja robaka internetowego, wykonywanie rozkazów przez bota), nastąpiło włamanie i przejęcie kontroli na komputerem lub świadome złośliwe działanie użytkownika. Wszystkie zgłoszenia ujęte w poniższych statystykach były przekazane automatycznie. W zestawieniu ujęto dane przysyłane przez naszych partnerów oraz pochodzące z naszych własnych systemów monitoringu. Dane te w większości trafiają do systemu n6 – platformy służącej do gromadzenia, przetwarzania i przekazywania informacji o zdarzeniach dotyczących bezpieczeństwa w sieci.

W roku 2012 zgłoszono nam 829 085 przypadków incydentów dotyczących 360 871 unikalnych adresów IP z Polski. Liczba zgłoszeń znacząco różni się od zeszłorocznej, która wynosiła ponad 5 mln. Wynika to głównie ze zmiany sposobu traktowania faktu zgłoszenia i liczenia zgłoszeń. Jeżeli dany adres IP był raportowany w danym dniu przez wielu naszych partnerów, jak również wykonywał w tym dniu ataki wielokrotnie (wiele adresów docelowych) czy na różne usługi (porty docelowe), to i tak zostało to potraktowane jako jeden incydent. Natomiast zgłoszenie z dnia następnego dotyczące tego samego adresu IP klasyfikowane już było w ramach nowego incydentu.

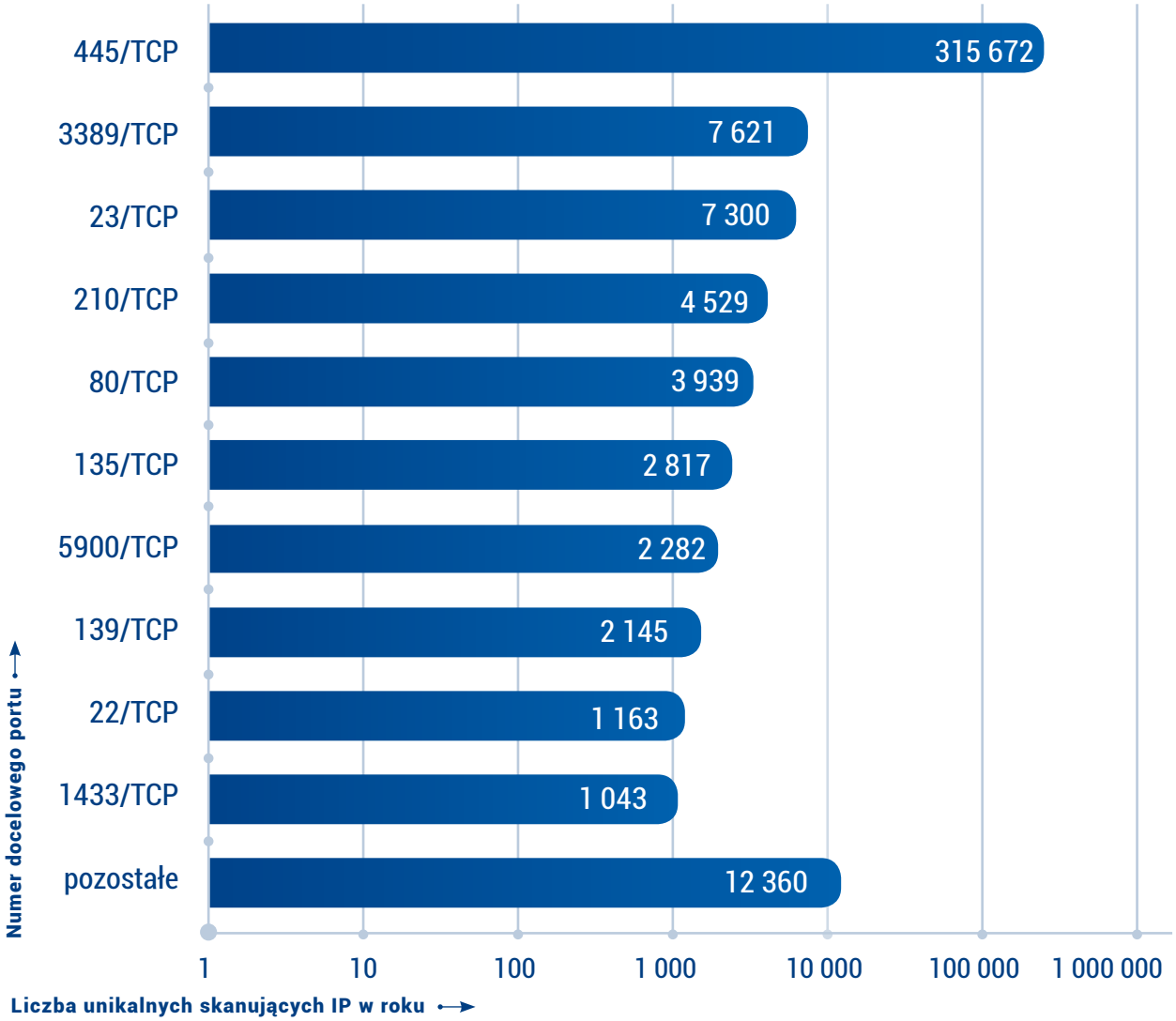
Ponadto na liczbę zgłoszeń mogły mieć wpływ zmiany partnerów przesyłających nam dane.

2.5.1 Najczęściej skanowane usługi

Poniżej przedstawiono statystyki dziesięciu najczęściej skanowanych portów docelowych pod kątem unikalnych w skali roku źródłowych adresów IP pochodzących z Polski. Ogólna liczba zgłaszanych unikalnych adresów IP zwiększyła się w stosunku do roku poprzedniego. **Uwaga! Na wykresie zastosowano skalę logarytmiczną!**

Pozycja	Liczba unikalnych IP	Port docelowy	Zmiana poz. w stosunku do 2011	Opis
1	315 672	445/TCP	0	Ataki typu buffer overflow na usługi Windows RPC
2	7 621	3389/TCP	▲ 8	Ataki słownikowe na RDP (zdalny pulpit)
3	7 300	23/TCP	▲ 3	Ataki na usługę telnet
4	4 529	210/TCP	nowość	Aplikacje wykorzystujące protokół Z39.50
5	3 939	80/TCP	0	Ataki na aplikacje webowe
6	2 817	135/TCP	▼ 4	Ataki na windowsową usługę DCE/RPC
7	2 282	5900/TCP	▲ 2	Ataki na VNC
8	2 145	139/TCP	▼ 5	Ataki na usługę NetBIOS / współdzielenie plików i drukarek
9	1 163	22/TCP	▼ 2	Ataki słownikowe na serwery SSH
10	1 043	1433/TCP	▼ 6	Ataki na MS SQL
11	12 360	pozostałe		inne

Tabela 6. Dziesięć najczęściej skanowanych portów docelowych pod kątem unikalnych w skali roku źródłowych adresów IP pochodzących z Polski



Rysunek 5. Dziesięć najczęściej skanowanych portów docelowych pod kątem unikalnych w skali roku źródłowych adresów IP pochodzących z Polski

Pierwsze miejsce w rankingu – podobnie jak w latach ubiegłych – zajmuje port 445/TCP. Większość najpoważniejszych, a więc najczęściej wykorzystywanych luk w systemach Windows znajduje się w usługach nasłuchujących na tym porcie. Wiele robaków wykorzystuje ten port do automatycznej propagacji. Stąd jego popularność względem pozostałych portów: liczba unikalnych adresów IP skanujących ten port wynosiła ponad 315 tys., co stanowi 70% liczby wszystkich unikalnych adresów IP znajdujących się w tej kategorii, podczas gdy na drugi w klasyfikacji port 3389/TCP łączyło się tylko 1,7% wszystkich unikalnych IP. Jednakże mimo znaczącej przewagi tego portu nad pozostałymi, to – podobnie jak w roku 2011 – jego procentowy udział zmalał.

Kolejne porty, na których domyślnie nasłuchują często atakowane usługi Windows – 135/TCP (usługa DCE/RPC), 139/TCP (NetBIOS, współdzielenie plików i drukarek) i 1433/TCP (serwer MS SQL) – z miejsc drugiego, trzeciego i czwartego spadły na odpowiednio szóste, ósme i dziesiąte. Nie oznacza to jednak, że usługi te są mniej atakowane – liczba unikalnych IP łączących się do nich nie zmieniła się znacząco w stosunku do roku 2011. Po prostu ataki na wszystkie pozostałe porty z rankingu zwiększyły się.

Na drugim miejscu w rankingu Top 10 znajduje port 3389/TCP z liczbą ponad 7,5 tys. unikalnych adresów IP. W roku 2011 znajdował się na 10. pozycji ze stosunkowo niewielką liczbą niemal 400 unikalnych adresów IP. Wzrost ataków na tym porcie jest więc znaczący. Port ten związany jest z usługą Windows Microsoft Terminal Server używającą protokołu RDP (wykorzystywany przez tzw. zdalny pulpit). Od sierpnia 2011 roku istnieje w sieci robak Morto, który poprzez tę usługę masowo infekował systemy Windows i propagował się dalej. Co ciekawe, Morto nie wykorzystuje żadnej luki, a jedynie odgaduje hasła użytkowników. Jednocześnie – poza aktywnością robaka Morto – obserwowaliśmy niezwiązane z robakiem próby łamania haseł w usłudze zdalnego pulpitu.

W rankingu Top 10 pojawił się nowy port w zestawieniu: 210/TCP, na którym domyślnie słucha usługa obsługująca protokół Z39.50 wykorzystywany powszechnie przez biblioteki do wymiany informacji w rozproszonych systemach bibliotecznych. Dodatkowo poza pierwszą dziesiątkę znalazł się port 25/TCP związany z protokołem SMTP.

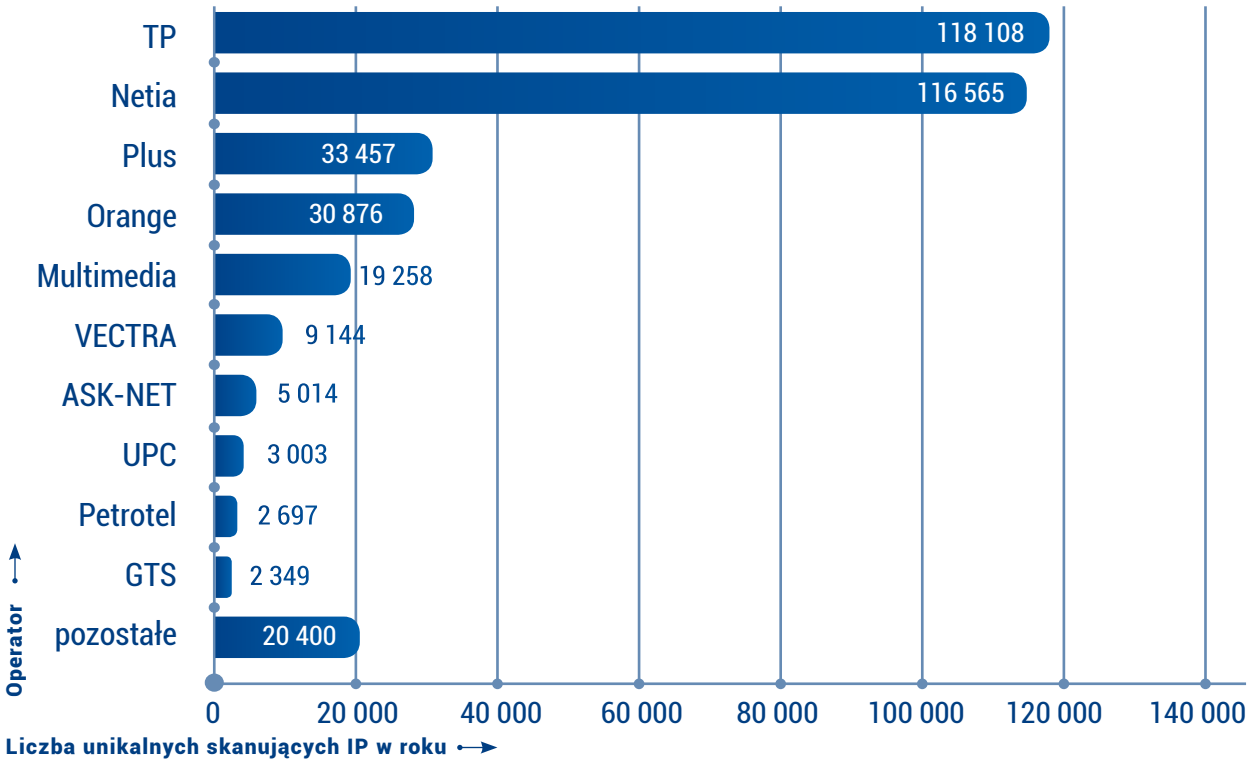
2.5.2 Polskie sieci

Najwięcej zgłaszanych do zespołu unikalnych w skali roku adresów IP z polskich sieci pochodziło – podobnie jak rok temu – z sieci TP (AS5617). Było to 118 tys. Stosunkowo niewiele mniej pochodziło z drugiej w rankingu sieci Netia (AS12741) – 116 tys. Rok temu TP i Netia również zajmowały dwie pierwsze pozycje, jednakże różnica między nimi była dużo większa. Trzecią z kolei polską siecią jest Plus (AS8374) z liczbą 33 tys. unikalnych adresów IP. Widać więc, że pomiędzy pierwszą dwójką a resztą sieci w rankingu jest znaczna różnica.

Poniżej przedstawiono ranking bezwzględny Top 10 sieci o największej liczbie unikalnych adresów IP zgłaszanych do naszego zespołu. W pierwszej dziesiątce pojawiła się – po rocznej przerwie – sieć UPC (AS6830) oraz Petrotel (AS29007) należący do Grupy Netia. Z rankingu wypadła sieć Dialog (AS15857), która w roku 2012 dołączyła do Grupy Netia, oraz T-Mobile (AS12912). We wszystkich sieciach znajdujących się w rankingu zwiększyła się liczba unikalnych adresów IP.

Pozycja	Liczba unikalnych w roku skanujących IP	Średnia liczba unikalnych skanujących IP na dzień	Numer AS	Nazwa operatora	Zmiana poz. w stosunku do 2011
1	118 108	612	5617	TP	0
2	116 565	532	12741	Netia	0
3	33 457	101	8374	Plus	▲ 2
4	30 876	101	43447	Orange	0
5	19 258	120	21021	Multimedia	▲ 1
6	9 144	134	29314	VECTRA	▲ 2
7	5 014	86	25388	ASK-NET	0
8	3 003	82	6830	UPC	nowość
9	2 697	16	29007	Petrotel	▲ 2
10	2 349	34	6714	GTS	▼ 1
	20 400			pozostałe	

Tabela 9. Ranking Top 10 sieci o największej liczbie unikalnych adresów IP zgłaszanych do CERT Polska

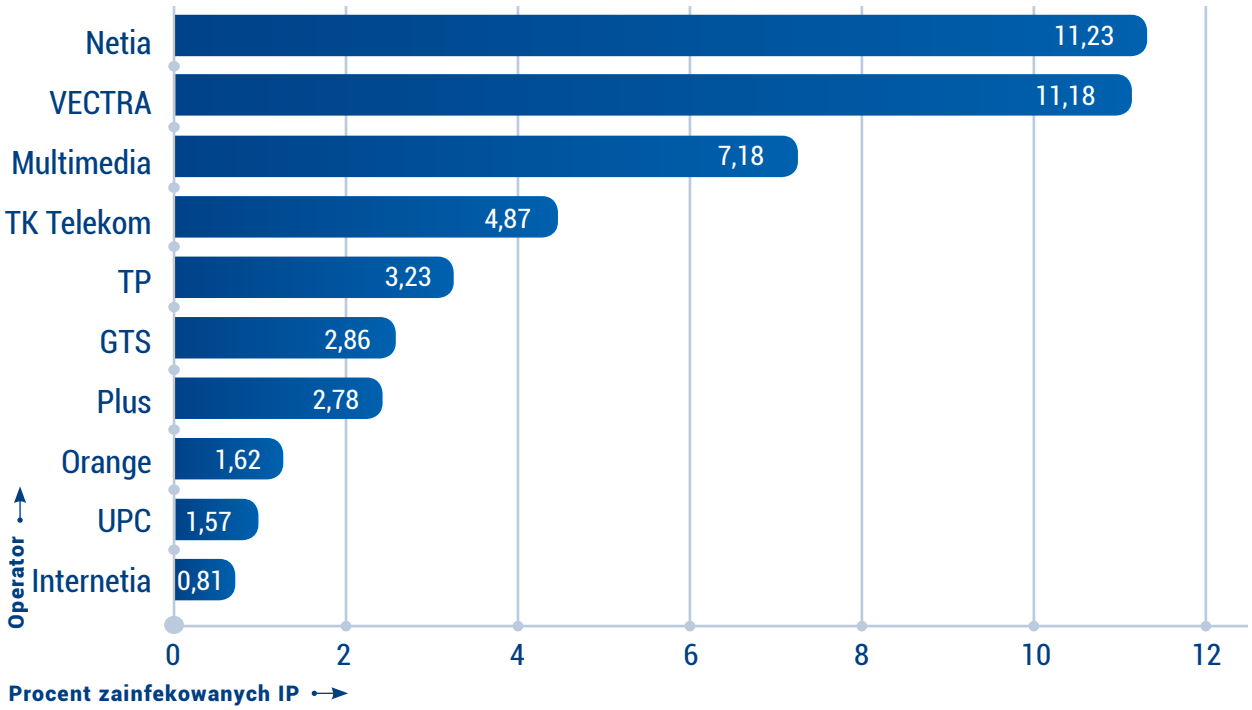


Rysunek 6. Ranking Top 10 sieci o największej liczbie unikalnych adresów IP zgłaszanych do CERT Polska

Wielkość systemu autonomicznego w przypadku powyższego rankingu bezwzględnego wpływa znacząco na pozycję dostawcy – im więcej adresów IP w sieci, tym większa liczba unikalnych skanujących adresów IP. Dlatego, podobnie jak w przypadku zainfekowanych unikalnych adresów IP, wprowadziliśmy jeszcze jedną statystykę uwzględniającą wielkość sieci. Został wprowadzony współczynnik opisujący procentowy udział unikalnych skanujących adresów IP w stosunku do wszystkich adresów IP należących do danego AS. W tym rankingu w pierwszej dziesiątce pojawiło się aż 5 sieci posiadających mniej niż 5 000 adresów IP oraz tylko jedna posiadająca więcej niż 250 000. Dlatego postanowiliśmy usunąć z rankingu wszystkie niewielkie sieci o rozmiarze do 250 000 adresów IP. W wyniku na pierwszym miejscu znalazła się sieć Netia (11,23% zainfekowanych IP), a przodująca w rankingu bezwzględnym sieć TP znalazła się na stosunkowo dalekim piątym miejscu (3,23% zainfekowanych IP). Ranking względny przedstawiono w tabeli poniżej.

Pozycja	Pocent zainfekowanych IP	ASN	Nazwa operatora	Pozycja w rankingu bezwzględnym
1	11,23	12741	Netia	2
2	11,18	29314	VECTRA	6
3	7,18	21021	Multimedia	5
4	4,87	20960	TK Telekom	14
5	3,23	5617	TP	1
6	2,86	6714	GTS	10
7	2,78	8374	Plus	3
8	1,62	43447	Orange	4
9	1,57	6830	UPC	8
10	0,81	43939	Internetia	19

Tabela 10. Ranking operatorów wg udziału unikalnych skanujących adresów IP w stosunku do wszystkich adresów IP należących do danego AS



Rysunek 7. Ranking operatorów wg udziału unikalnych skanujących adresów IP w stosunku do wszystkich adresów IP należących do danego AS

Poniżej przedstawiamy statystyki dotyczące najczęściej skanowanych portów docelowych w poszczególnych sieciach. Pod uwagę wzięliśmy tylko sieci z bezwzględnego rankingu Top 10.

	TP		Netia		Plus		Orange		Multimedia	
1	445/TCP	67,9%	445/TCP	83,7%	445/TCP	96,5%	445/TCP	95,4%	445/TCP	81,6%
2	3389/TCP	3,5%	139/TCP	1,1%	161/UDP	0,6%	5900/TCP	0,5%	135/TCP	2,5%
3	23/TCP	2,4%	23/TCP	1,1%	143/TCP	0,3%	23/TCP	0,3%	23/TCP	1,0%
	pozostałe	26,2%	pozostałe	14,1%	pozostałe	2,7%	pozostałe	3,8%	pozostałe	14,9%

	Vectra		ASK-NET		UPC		Petrotel		GTS	
1	445/TCP	71,6%	445/TCP	90,6%	445/TCP	16,8%	445/TCP	95,2%	445/TCP	54,1%
2	3389/TCP	1,6%	139/TCP	0,7%	23/TCP	8,6%	3389;6	0,5%	23/TCP	2,3%
3	23/TCP	1,1%	135/TCP	0,5%	139/TCP	3,5%	23;6	0,5%	210/TCP	1,6%
	pozostałe	25,8%	pozostałe	8,2%	pozostałe	71,1%	pozostałe	3,8%	pozostałe	42,0%

Tabela 11. Ranking najczęściej skanowanych portów docelowych w poszczególnych sieciach (tylko sieci z bezwzględnego rankingu Top 10)

2.6 Strony związane ze złośliwym oprogramowaniem

W roku 2012 zanotowaliśmy 229 901 linków w domenie .pl, które zawierały złośliwą zawartość. Jako „złośliwą zawartość" należy rozumieć złośliwe oprogramowanie, złośliwe Java Scripty bądź iframe'y wyświetlające zawartość z innych serwerów.

2.6.1 Domeny pl. zawierające najwięcej złośliwych linków.

Najwięcej złośliwych linków odnotowaliśmy w domenie katalog.onet.pl. W tym przypadku sytuacja jest nieco skomplikowana i wymaga kilku słów wytłumaczenia. Katalog.onet.pl jest wyszukiwarką stron www znajdujących się zazwyczaj poza sieciami serwisu. Wyniki wyświetlane przez Onet same w sobie nie zawierają złośliwej zawartości, za to zawierały ją znajdowane strony. Fakt ten spowodował ich pojawienie się w rankingu. Należy zwrócić uwagę, że katalog jest bezpieczny, ale odwiedzenie stron będących wynikiem wyszukiwania może zakończyć się infekcją komputera.

Pozostałe nazwy, za wyjątkiem **www.vodca.pl**, były prawdopodobnie wykorzystywane do hostowania stron reklamowych. Rozpatrujemy dwa scenariusze: same strony zawierały złośliwą zawartość, bądź znajdowały się na nich linki do złośliwych stron. W przypadku **www.vodca.pl** wydaje się, że miało miejsce włamanie i doklejono kod do stron.

LP	Domena	Liczba unikalnych złośliwych linków
1	katalog.onet.pl	7 426
2	www.przepisane.ilawa.pl	2 531
3	cudownystyl.pl	1 993
4	www.numery.pwy.pl	1 921
5	outlet1st.za.pl	1 839
6	www.helweg.waw.pl	1 701
7	www.vodca.pl	1 498
8	super-zdrowo.pl	1 440
9	adamantczak.friko.pl	1 326
10	valenciaswigert.w8w.pl	1 193

Tabela 12. Liczba unikalnych złośliwych linków występujących w domenie .pl

2.6.2 Adresy IP, na których znajdowało się najwięcej złośliwych linków

Najwięcej złośliwych linków znajdowało się pod adresem IP 217.74.66.183. Wszystkie były się na stronach WWW umieszczonych w hostingu należącym do Interia.pl i zawierały się w domenie strefa.pl

W przypadku kolejnych adresów mamy również do czynienia z firmami hostingowymi i stronami ich klientów. Pojawienie się IP 213.180.146.24 jest wynikiem opisanego powyżej przypadku katalogu Onetu. IP 194.9.24.158 to nic innego jak strony znajdujące się w domenie prv.pl. IP 213.180.150.17, to w większości strony hostowane w domenie republika.pl. IP 66.96.221.165 to strony z domen osa.pl, bee.pl oraz orge.pl.

LP	IP	AS	Liczba unikalnych złośliwych linków
1	217.74.66.183	INTERIAPL	24 702
2	213.180.146.24	ONET-PL-AS1	7 426
3	194.9.24.158	CRMEDIA-AS	6 234
4	178.19.104.228	LIVENET-PL	4 941
5	213.180.150.17	ONET-PL-AS1	3 725
6	94.23.93.10	OVH	3 545
7	94.23.93.156	OVH	2 536
8	66.96.221.165	NOC	2 387
9	94.23.95.68	OVH	2 206
10	188.40.38.212	HETZNER-AS	2 026

Tabela 13. Liczba złośliwych linków znajdujących się na jednym adresie IP

2.6.3 Systemy autonomiczne, w których było najwięcej złośliwych linków

AS-y, w których znalazły się złośliwe linki, należą do dużych firm hostingowych. Ciekawy jest fakt, że na dwóch pierwszych miejscach znalazły się AS-y umiejscowione poza granicami kraju, kolejno - OVH we Francji i Hetzner w Niemczech. Jest to efekt dość dużej popularności tych hostingów. W pierwszej dziesiątce z zagranicznych podmiotów znalazł się jeszcze holenderski Leaseweb. Resztę listy tworzą największe polskie hostingi, takie jak Interia, Home, NetArt czy Onet.

LP	Numer AS	Właściciel AS	Liczba unikalnych złośliwych linków
1	16276	OVH	38 216
2	24940	HETZNER-AS	29 624
3	16138	INTERIAPL	27 583
4	12824	HOMEPL-AS	19 957
5	15967	NETART	12 391
6	12990	ONET-PL-AS1	11 181
7	59491	LIVENET-PL	10 401
8	16265	LEASEWEB	6 944
9	41406	CRMEDIA-AS	6 635
10	196763	KEY-SYSTEMS-AS	5 796

Tabela 14. Liczba unikalnych złośliwych linków występujących w AS

2.6.4 Rozkład geograficzny złośliwych linków w domenie .pl

Większość złośliwych stron z domeny .pl była zamieszczona na serwerach w Polsce, które znajdowały się w sieciach dużych firm hostingowych. Strony w Niemczech były umieszczone głównie na serwerach należących do Hetznera, zaś te znajdujące się we Francji - do OVH.

LP	Kraj	Liczba unikalnych złośliwych linków
1	PL	137 681
2	DE	40 078
3	FR	38 216
4	NL	6 982
5	US	5 010
6	CZ	1 055
7	GB	336
8	EU	134
9	RU	120
10	CA	80
11	AT	79
12	CH	51
13	ES	27
14	IT	16
15	SE	8
16	LT	8
17	IE	7
18	DK	6
19	HU	2
20	FI	2
21	VN	1
22	RO	1
23	BG	1

Tabela 15. Rozkład geograficzny złośliwych linków, hostowanych w domenie .pl

2.7 Ataki brute-force

Ataki zwane "brute-force" związane są z próbami uzyskania dostępu przez użycie domyślnych haseł, błędów w konfiguracji lub podatności w implementacji funkcji logowania.

W roku 2012 otrzymaliśmy 64 250 zgłoszeń dotyczących ślepych prób logowania się do usług. Jest to mniej niż połowa tego, co zostało nam zgłoszone w roku 2011. Wszystkie zgłoszenia dotyczyły prób logowania do usługi SSH (domyślny port: 22/TCP). Ich liczba nie odpowiada jednak zdecydowanie skali problemu. Próby pochodziły bowiem jedynie ze 112 unikalnych adresów IP w skali roku (liczba podobna jak w roku 2011). W statystykach skanowań (rozdział 2.5) port 22/TCP występuje dosyć wysoko, a więc popularność ataków na usługę SSH wcale nie jest mała. Oznacza to, że najprawdopodobniej stosunkowo niewiele prób logowania do SSH jest zgłaszanych jako ataki brute-force - częściej zgłaszane są jako

skanowania. Być może wynika to z narzędzi służących do monitorowania ruchu i wykrywania ataków - tylko w przypadku użycia honeypotów wysokointeraktywnych lub specjalizowanych, ewentualnie obserwacji produkcyjnego serwera SSH, istnieje pewność, że był to brute-force. W pozostałych przypadkach (jak użycie honeypotów niskointeraktywnych, niespecjalizowanych lub poleganie tylko na informacjach o połączeniach zablokowanych przez zaporę sieciową) - ewentualne ataki brute-force mogły jedynie zostać sklasyfikowane jako skanowanie.

Najwięcej zgłoszeń - ponad 2 000 - otrzymaliśmy w lutym. Dotyczyły one zaledwie 16 adresów. Oznacza to, że z niewielkiej liczby adresów przeprowadzono stosunkowo dużo ataków. Najwięcej unikalnych (zarówno na dzień, jak i w skali miesiąca) adresów IP zostało zgłoszonych w kwietniu, natomiast najbardziej spokojnie (najmniej zgłoszeń oraz unikalnych IP) było w lipcu.

2.8 Adresy odwiedzane przez złośliwe oprogramowanie

Uruchamianie plików wykonywalnych w kontrolowanym środowisku (ang. sandbox) i monitorowanie jego zachowania jest jedną z podstawowych metod automatycznej analizy podejrzanego oprogramowania. Dzięki tej technice można uzyskać szeroki zakres informacji o badanych programach, w szczególności ustalić czy bez interakcji użytkownika łączą się do zdalnych serwerów, co może być efektem złośliwej aktywności. W tej kategorii incydentów uwzględniamy wszystkie przypadki połączenia się przez podejrzany program z serwerem znajdującym się w Polsce.

W poprzednich latach informacje o tego rodzaju połączeniach otrzymywaliśmy wyłącznie ze źródeł zewnętrznych. Jednak na początku roku 2012 uruchomiliśmy produkcyjnie własny system do automatycznej analizy oprogramowania który, pozwala na samodzielny wybór badanych plików. Wszystkie statystyki przedstawione dalej odnoszą się do złączonych danych ze źródeł zewnętrznych oraz pozyskanych z systemu wewnętrznego.

Tabela 16 zawiera zestawienie 10 domen, do których łączyła się największa liczba analizowanych programów. Z naszej analizy wynika, że większość z najczęściej występujących adresów, w szczególności w domenach `benjaminstrahs.com`, `filesfrog.com` i `etype.com`, była wykorzystywana do pobrania oprogramowania typu adware (wyświetlającego niechciane reklamy) lub spyware (wysyłającego dane użytkownika bez jego wiedzy). W zestawieniu pojawiają się również kontrolery botnetów (serwery command & control), takie jak `pelcpawel.fm.` `interia.pl`, czy `gim8.pl` oraz adresy IP do których boty łączą się bezpośrednio po adresach IP, m.in. `79.96.81.234`, `192.166.218.217 i 192.166.218.218`. Niektóre ze wspomnianych adresów, w szczególności `pelcpawel.fm.interia.pl`, już od kilku lat nie funkcjonują jako kanały komunikacji z kontrolerami, ale wciąż rozpowszechnione jest złośliwe oprogramowanie, które się do nich łączy.

Często autorzy złośliwego oprogramowania używają serwisów oferujących darmowe poddomeny do rejestracji adresów, które następnie służą do komunikacji z kontrolerem botnetu, ściągania plików zawierających trojany, itp. Po sprawdzeniu, jak pełne nazwy domenowe rozkładają się względem domen drugiego poziomu, okazało się, że zdecydowanie najczęściej do rejestracji używany był serwis osa.pl, w którym znalazło się 640 zaobserwowanych przez nas unikalnych poddomen. Kolejne miejsca w rankingu liczby poddomen zajmuje home.pl z 36 oraz interia.pl z 19 adresami.

domena / adres IP	programy
download.benjaminstrahs.com	4 293
pelcpawel.fm.interia.pl	1 732
www.bee.pl	768
gim8.pl	552
79.96.81.234	516
download.filesfrog.com	478
software.filesfrog.com	443
192.166.218.218	429
version.etype.com	400
192.166.218.217	378

Tabela 16. Domeny najczęściej odwiedzane przez złośliwe oprogramowanie

2.9 Phishing

Phishing w Polsce

W 2012 roku otrzymaliśmy 5 335 zgłoszeń przypadków phishingu w polskich sieciach. Dotyczyły one 2 576 adresów URL w 1 026 domen, w tym 673 z końcówką .pl.

W odróżnieniu od ubiegłego roku nie pojawił się problem masowej rejestracji darmowych poddomen z końcówką .pl w serwisach oferujących takie usługi. Praktycznie we wszystkich przypadkach phishing na adresach z końcówką .pl był skutkiem włamania.

Spośród 353 pozostałych domen aż jedną trzecią (120) stanowiła seria nazw z końcówkami .org, .net, .eu i .biz, rejestrowanych prawdopodobnie przez jedną grupę. Do phishingu wykorzystywano w nich zawsze subdomeny złożone z sześciu cyfr, być może stanowiących identyfikator konkretnej kampanii. Przykładowy adres: 953959.master-formular-bestaetigungen.biz. Wnioskując z nazw, strony te służyły najprawdopodobniej wyłudzaniu danych użytkowników serwisu PayPal oraz właścicieli kart Mastercard z Niemiec. Utrzymywane były w sieciach różnych dostawców. Czasem także zmieniały lokalizację.

W Tabeli 17 znajduje się rozkład liczby zgłoszeń dotyczących polskich sieci w zależności od systemu autonomicznego. Nie powinna zaskakiwać wysoka pozycja dwóch największych dostawców usług hostingu, ponieważ phishing umieszczany jest zazwyczaj albo na wykupionych w tym celu usługach, albo – znacznie częściej – w wyniku włamania na zwykłe serwisy WWW niewielkich firm czy instytucji, które w przeważającej części korzystają z usług hostingu.

	ASN	Nazwa	Liczba zgłoszeń phishingu	IP	URLs	Liczba zgłoszeń / IP
1	12824	Home.pl	1153	176	621	6,55
2	15967	NetArt	779	140	426	5,56
3	41079	Superhost	339	19	172	17,84
4	5617	TP S.A.	294	52	150	5,65
5	21021	Multimedia	272	19	134	14,32
6	15694	ATM S.A.	234	12	141	19,50
7	12741	Netia S.A.	167	25	100	6,68
8	49792	IONIC	140	7	72	20,00
9	29522	KEI	137	15	78	9,13
10	43333	CIS NEPHAX	97	16	52	6,06

Tabela 17. Liczba przypadków tradycyjnego phishingu według systemów autonomicznych

Ostatnia kolumna informuje o stosunku liczby zgłoszeń do unikalnych adresów IP, których dotyczyły. Pozwala to wstępnie oszacować, jak długo strony phishingowe utrzymywały się w danym systemie autonomicznym – im mniej zgłoszeń na jeden adres, tym szybciej usuwane były strony.

Polska a świat

Przeanalizowaliśmy 342 091 zgłoszeń dotyczących całego świata, aby przyjrzeć się globalnemu obrazowi tradycyjnego phishingu. Nie braliśmy pod uwagę źródeł, które ograniczają się do informacji o Polsce, aby mieć możliwość obiektywnego porównania poszczególnych krajów. W Tabeli 18 przedstawiamy rozkład liczby zgłoszeń według krajów, w których znajdowała się strona (kryterium jest geolokalizacja adresu IP, nie adres domenowy). Rozkład nie różni się znacząco od zeszłorocznego. Dominującą pozycję zajmują niezmiennie Stany Zjednoczone, co tłumaczymy dostępnością tanich usług hostingu. Jedyną niespodzianką jest wysoka pozycja Australii, przy czym duża bezwzględna liczba zgłoszeń dotyczy stosunkowo niewielkiej liczby adresów IP oraz URL, co wskazuje na pewne problemy z szybkim usuwaniem phishingu w Australii. Struktura adresów australijskich stron phishingowych wskazuje na to, że w kilku przypadkach dochodziło do włamania na pojedyncze serwisy, na których umieszczano bardzo wiele stron phishingowych, zapewne za pomocą gotowych narzędzi.

Polska zajmuje stosunkowo niską piętnastą pozycję, z identycznym jak w zeszłym roku udziałem 0,8% w ogólnej liczbie zgłoszeń. (Liczba 2 675 wynika z pominięcia niektórych źródeł, o czym napisaliśmy wcześniej.)

Pozycja	kraj	liczba zgłoszeń	Procentowy udział w zgłoszeniach	liczba unikalnych URL	liczba unikalnych IP
1	US	164 850	49,0%	136 850	22 637
2	AU	15 482	4,6%	7 327	544
3	DE	15 073	4,5%	12 616	3 099
4	GB	13 646	4,1%	11 792	1 776
5	CN	13 081	3,9%	1 004	1 452
6	CA	12 001	3,6%	10 654	1 132
7	FR	10 941	3,2%	9 298	1 462
8	BR	10 075	3,0%	9 062	2 031
9	RU	6 794	2,0%	5 667	1 102
10	CZ	6 126	1,8%	4 259	260
15	**PL**	**2 675**	**0,8%**	**2 140**	**654**

Tabela 18. Liczba zgłoszeń tradycyjnego phishingu według krajów

2.10 Serwery command & control

W 2012 roku zarejestrowaliśmy 137 przypadków umieszczenia serwera zarządzającego siecią botnet (czyli tzw. serwera C&C) pod adresem IP w polskiej sieci. To ponad dwukrotnie więcej niż w 2011 roku, przede wszystkim ze względu na uwzględnienie nowych źródeł informacji. Z tej samej przyczyny odstąpiliśmy od zliczania wszystkich zgłoszeń (w roku 2011 w tej kategorii było ich 2 263) – część źródeł nie zaprzestaje raportowania nawet po ustaniu aktywności kontrolera, więc uwzględnienie ich powodowałoby niemiarodajność informacji.

Tabela 19 pokazuje rozkład liczby wykrytych serwerów C&C według systemów autonomicznych:

Liczba C&C	Numer AS	Operator
21	5 617	TPNET Telekomunikacja Polska S.A.
13	21 021	MULTIMEDIA-AS Multimedia Polska S.A.
11	6 830	LGI-UPC Liberty Global Operations B.V.
7	12 741	INTERNETIA-AS Netia SA
7	12 824	HOMEPL-AS home.pl Sp. z o.o.
6	29 314	VECTRANET-AS VECTRA S.A.
72	inne	inne

Tabela 19. Systemy autonomiczne polskich operatorów, w których najwięcej znajdowały się serwery C&C

W porównaniu do ubiegłego roku zwraca uwagę brak dużych hostowni, dominujących zestawienie z 2011 roku. W polskich sieciach należących do OVH i LEASEWEB znalazł się w tym roku tylko jeden adres IP kontrolera botnetu. Przyczyna takiego obrazu może być jednak prozaiczna – zmiany w opisach sieci tych dostawców i administracyjnym przyporządkowaniu ich do poszczególnych krajów.

Oprócz serwerów C&C utrzymywanych w sieciach IP polskich operatorów, mieliśmy do czynienia także z wieloma przypadkami wykorzystywania polskich domen (same serwery znajdowały się przy tym często w innych krajach). Piszemy o tym szerzej w rozdziale 2.8.

2.11 Pozostałe zgłoszenia

Pozostałe automatyczne zgłoszenia w liczbie 13 031 dotyczyły przede wszystkim błędów w konfiguracjach urządzeń, umożliwiających tworzenie anonimowych połączeń proxy, błędów dotyczących konfiguracji routerów, a także pojedynczych przypadków ataków DDoS. W przypadku tych ostatnich chodzi jedynie o te ataki, które zostały przeprowadzone z wykorzystaniem monitorowanych serwerów C&C. Było ich zbyt mało aby wykonywać na ich podstawie porównania czy analizy. Większa liczba ataków DDoS została zgłoszona do nas indywidualnie i znalazła odzwierciedlenie w statystykach w rozdziale 3. Rozdział 4.1 poświęciliśmy natomiast opisowi styczniowych ataków DDoS firmowanych przez grupę Anonymous.

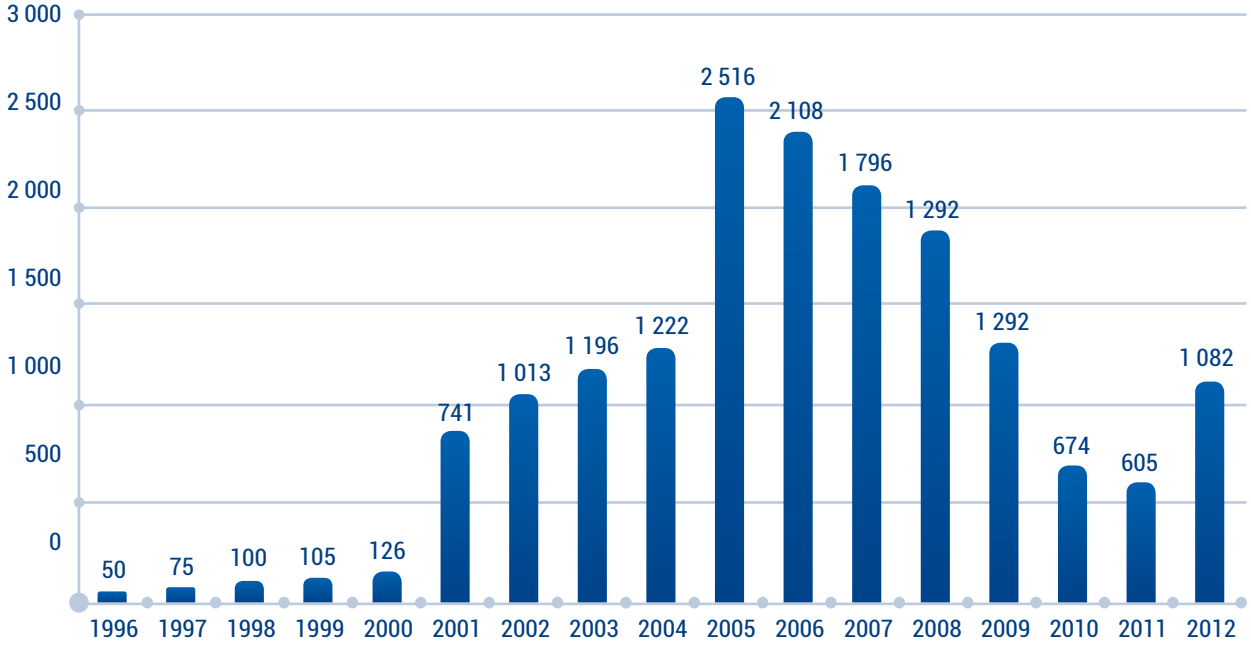
W przypadku pozostałych zagrożeń zarówno ich skala jak i poziom ich istotności także nie uzasadniają ich szczegółowego opisywania w niniejszym raporcie tym bardziej, że nie zaobserwowaliśmy żadnych wyraźnych trendów.

3 Statystyka incydentów obsłużonych przez CERT Polska

W tej części raportu prezentujemy opracowane przez CERT Polska statystyki otrzymanych przez zespół zgłoszeń, zarówno ze źródeł zewnętrznych, jak i z wewnętrznych, własnych systemów.

Ręcznie obsłużone incydenty i trendy

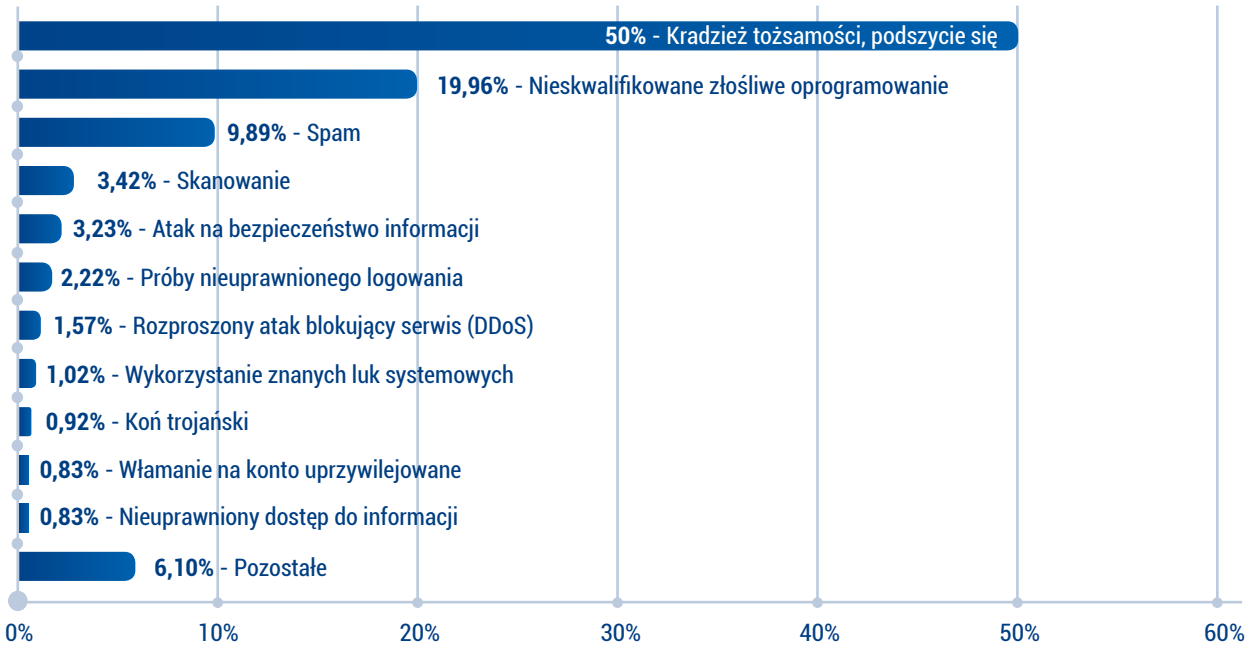
W 2012 roku zespół CERT Polska obsłużył ręcznie 1 082 incydenty. Tak jak w latach poprzednich większość z nich stanowiły te dotyczące phishingu (ok. 50%), złośliwego oprogramowania (ok. 20%) oraz spamu (prawie 10%). Zgłaszającym, poszkodowanym i atakującym były głównie firmy komercyjne (kolejno 53,8%, 59,6%, 75,7%). Zgłaszający i poszkodowany pochodził zazwyczaj z zagranicy (78,8% oraz 54,4%), a atakujący pozostawał nieznany w 78,7% przypadków.



Rysunek 8. Liczba incydentów 1996-2012

			%	%
Obraźliwe i nielegalne treści	**5**	**114**	**0,50**	**10,54**
Spam	107		9,89	
Dyskredytacja, obrażanie	0		0,00	
Pornografia dziecięca, przemoc	2		0,18	
Złośliwe oprogramowanie	**216**	**226**	**19,96**	**20,89**
Wirus	0		0,00	
Robak sieciowy	0		0,00	
Koń trojański	10		0,92	
Oprogramowanie szpiegowskie	0		0,00	
Dialer	0		0,00	
Gromadzenie informacji	**4**	**41**	**0,37**	**3,79**
Skanowanie	37		3,42	
Podsłuch	0		0,00	
Inżynieria społeczna	0		0,00	
Próby włamań	**9**	**44**	**0,83**	**4,07**
Wykorzystanie znanych luk systemowych	11		1,02	
Próby nieuprawnionego logowania	24		2,22	
Wykorzystanie nieznanych luk systemowych	0		0,00	
Włamania	**4**	**14**	**0,37**	**1,29**
Włamanie na konto uprzywilejowane	9		0,83	
Włamanie na konto zwykłe	1		0,09	
Włamanie do aplikacji	0		0,00	
Dostępność zasobów	**0**	**25**	**0,00**	**2,31**
Atak blokujący serwis (DoS)	8		0,74	
Rozproszony atak blokujący serwis (DDoS)	17		1,57	
Sabotaż komputerowy	0		0,00	
Atak na bezpieczeństwo informacji	**35**	**44**	**3,23**	**4,07**
Nieuprawniony dostęp do informacji	9		0,83	
Nieuprawniona zmiana informacji	0		0,00	
Oszustwa komputerowe	**13**	**559**	**1,20**	**51,66**
Nieuprawnione wykorzystanie zasobów	0		0,00	
Naruszenie praw autorskich	5		0,46	
Kradzież tożsamości, podszycie się	541		50,00	
Inne	**15**	**15**	**1,39**	**1,39**

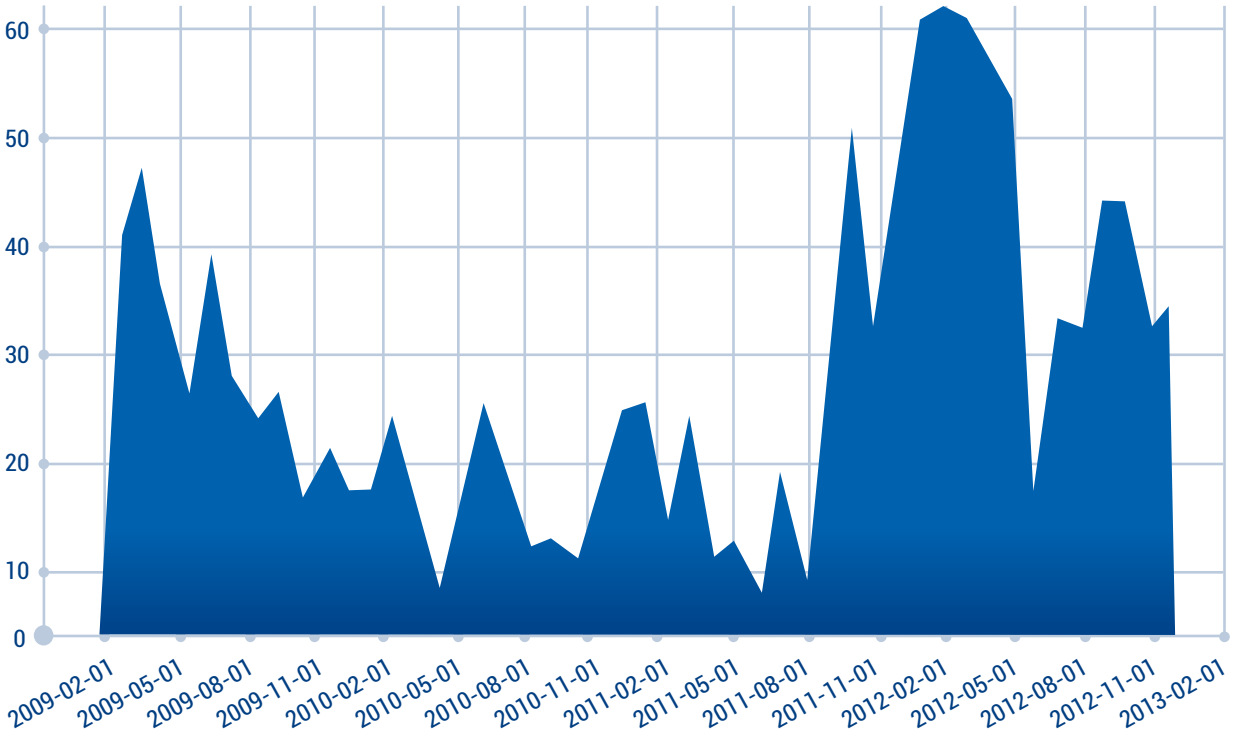
Tabela 20. Incydenty obsłużone przez CERT Polska wg typów



Rysunek 9. Rozkład procentowy podtypów incydentów

W związku z faktem, że statystyki liczone w oparciu o udział procentowy poszczególnych incydentów wyglądają niemal identycznie od kilku lat, pokusiliśmy się o porównanie wartości bezwzględnych na przestrzeni ostatnich 4 lat. Oto najciekawsze wnioski wynikające z tego porównania:

- pod koniec 2011 roku znacznie wzrosła liczba incydentów dotyczących phishingu. Od 2010 do sierpnia 2011 roku notowaliśmy poniżej 30 incydentów miesięcznie, następnie liczba ta wzrosła dwukrotnie do ponad 60 incydentów.



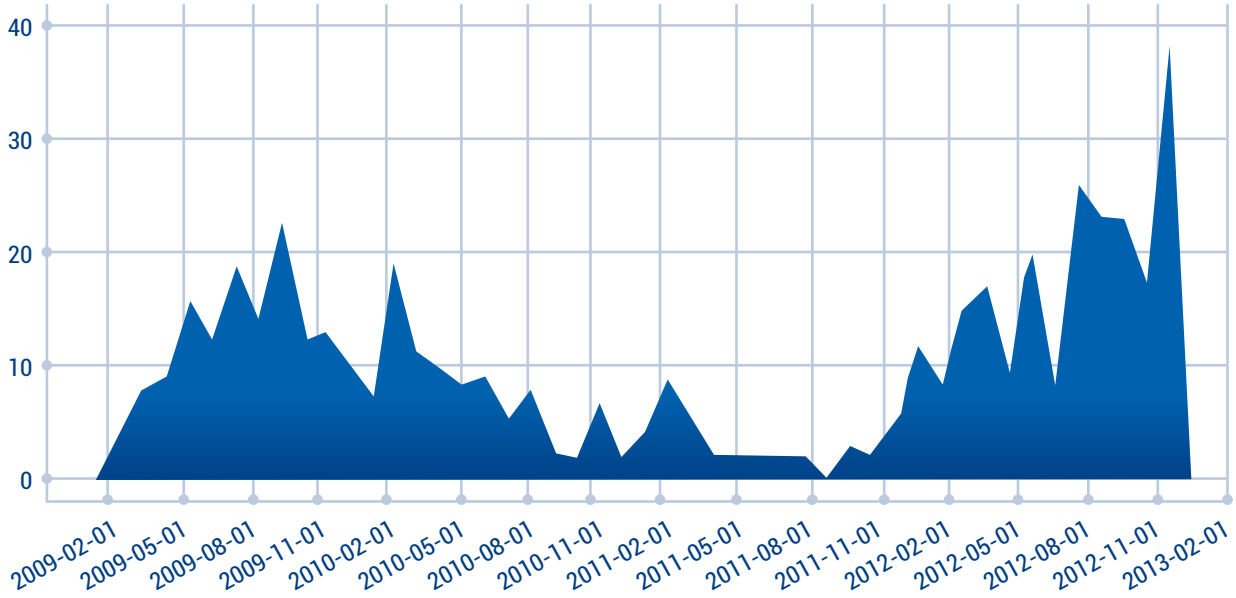
Rysunek 10. Liczba incydentów dotyczących phishingu na przestrzeni ostatnich 4 lat

- w 2012 roku znacznie wzrosła liczba incydentów dotyczących złośliwego oprogramowania. Zauważalny jest trend rosnący na przestrzeni całego roku. W głównej mierze incydenty dotyczące złośliwego oprogramowania przełożyły się na wzrost liczby incydentów obsłużonych w 2012 roku.

- od połowy 2010 roku rośnie liczba poszkodowanych firm komercyjnych z zagranicy. W 2010 roku było ich ok. 200, zaś w 2012 prawie 500. Jest to w dużej mierze wynik phishingu dotyczącego tych firm, który był umieszczony na polskich serwerach.

- zmalała liczba zagranicznych zgłoszeń dotyczących spamu, głównie za przyczyną zgłoszeń od innych instytucji ds. bezpieczeństwa - z ponad 300 incydentów w roku 2009 do mniej niż 100 w 2012 roku.

- znacznie spadła liczba zgłoszeń od osób prywatnych z Polski, szczególnie w przypadku incydentów dotyczących spamu i phishingu.

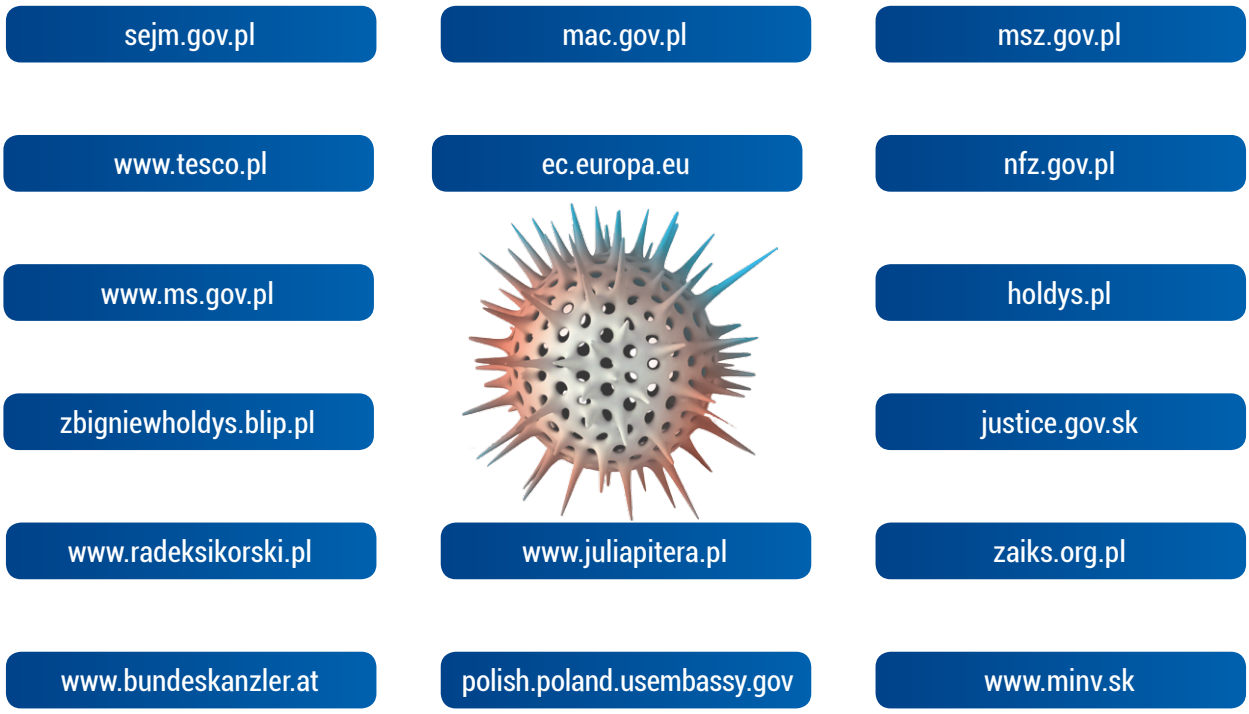


Rysunek 11. Liczba incydentów dotyczących złośliwego oprogramowania na przestrzeni ostatnich 4 lat

4 Najważniejsze zjawiska okiem CERT Polska

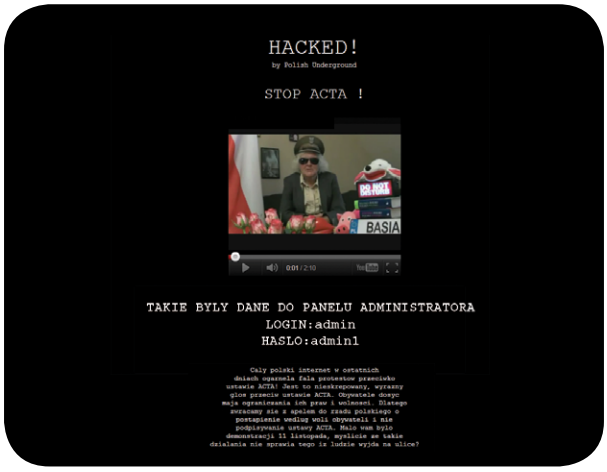
4.1 Ilość informacji we wszystkich kategoriach

Pod koniec stycznia 2012 roku obserwowaliśmy serię ataków na serwisy rządowe, związane z falą protestów przeciw zapowiedziom podpisania przez Polskę porozumienia ACTA. Do ataków tych nawoływała za pośrednictwem mediów społecznościowych grupa Anonymous Polska, zachęcając do blokowania dostępu do witryn resortów odpowiedzialnych za prace nad ACTA, a więc przede wszystkim Ministerstwa Administracji i Cyfryzacji, Ministerstwa Spraw Zagranicznych, Sejmu RP i Kancelarii Premiera. Na wielu stronach internetowych publikowano narzędzia (LOIC i HOIC) służące do seryjnego generowania zapytań do zdefiniowanych witryn. Akcja koordynowana była także na dedykowanych kanałach IRC. Ataki trwały około tygodnia, pomiędzy 21 a 28 stycznia i w wielu przypadkach były skuteczne. Według analiz przeprowadzonych przez CERT Polska, ruch odpowiedzialny za blokowanie serwisów pochodził w większości z Polski. Świadczy to o tym, że znaczący wpływ mieli internauci korzystający z narzędzi takich jak LOIC, działających po stronie klienta, a nie ruch pochodzący z botnetów, często wykorzystywanych przy tego rodzaju atakach.



Warto przy tym zauważyć, że zarówno pobudki jak i wiedza techniczna osób przeprowadzających ataki pod wpływem zachęt Anonimowych, pozostawiały wiele do życzenia. Piszemy o tym w artykule **http://www.cert.pl/news/4856**. Łącznie ofiarami ataków padło kilkanaście różnych domen, często w żaden sposób niezwiązanych z ACTA (np. tesco.pl).

Oprócz ataków DDoS, w kilku przypadkach doprowadzono do skutecznej podmiany zawartości stron, w tym Kancelarii Premiera oraz MON.



Rysunek 12. Witryna Premiera RP z podmienioną zawartością

4.2 „Polowanie na muły"

W 2012 roku odbyło się kilka kampanii mających na celu rekrutację osób transferujących środki pieniężne. Pieniądze te zazwyczaj pochodzą z kradzieży internetowych kont bankowych.

Przestępcy poszukują osób, które umożliwią im przetransferowanie skradzionych pieniędzy, najlepiej poprzez przekazy pieniężne. Zrekrutowane osoby powinny liczyć się z tym, że mogą zostać posądzone o współudział w kradzieży. Gdy skradzione środki wędrują przez kilka krajów, dochodzenie staje się bardziej skomplikowane, wymaga konieczności kontaktu organów ścigania z różnych państw, co znacznie wydłuża śledztwo. Aby spróbować oszacować skalę zjawiska, warto przytoczyć sprawę MoneyGram. W listopadzie 2012 roku MoneyGram, jedna z największych firm operująca w obszarze przekazów pieniężnych, zgodziła się zapłacić 100 milionów dolarów ugody w wyniku oskarżenia przez amerykański Departament Sprawiedliwości o niewystarczające starania przy przeciwdziałaniu praniu brudnych pieniędzy. Kwota ta została oszacowana jako minimum zdefraudowanych pieniędzy za pośrednictwem MoneyGram w latach 2004 – 2009.

"Kradzież tożsamości"

Pierwsza duża kampania rekrutująca pośredników miała miejsce w lutym 2012 roku. Jej najciekawszym aspektem było wykorzystanie wizerunku firmy Magellan Pertoleum Corporation. Do internautów wysłane zostały wiadomości zawierające spam o następującej treści (pisownia oryginalna):

> Szanowni Panstwo!
> Wydzial Magellan Petroleum Corporation, duzej miedzynarodowej firmy, przyjmuje aplikacje na stanowisko w swoim dziale Kontroli Kredytowej dla Europy Wschodniej. Obecnie potrzebujemy pracownikow w terenie, poniewaz nasz wydzial rozprowadza produkty firmy w krajach europejskich.
>
> Dzieki poprawie koniunktury po kryzysie ekonomicznym co raz wiecej duzych firm zatrudnia pracownikow do pracy zdalnej. Praca zdalna w znaczacym stopniu obniza koszty utrzymania przestrzeni biurowej w budzecie firmy, a pracownicy nie maja potrzeby codziennego dojazdu do biura. W nowoczesnym swiecie technologii informacyjnej jest to ekonomiczne rozwiazanie, ktore uwalnia fundusze dla wzrostu firmy i pozwala na godziwe wynagradzanie pracownikow.
>
> Obecnie poszukujemy agentow terenowych, ktorych zadaniem bedzie kontrola platnosci pomiedzy nasza firma a klientami w krajach europejskich, ktore nie sa czlonkami strefy euro. Potrzeba ta wynikla z faktu, ze realizacja przelewow internetowych zajmuje duzo czasu i nie posiadaja one wystarczajacego poziomu zabezpieczen przed kradzieza naszych funduszy. Z tego powodu kontrolujemy oplaty za pomoca agentow. Do obowiazkow agenta nalezy wykonywanie przelewow bankowych oraz dokonywanie biezacych przelewow srodkow za pomoca miedzynarodowych systemow platnosci. Plan pracy agenta musi byc wystarczajaco elastyczny, aby umozliwic mu kontrole srodkow przychodzacych na konto w ciagu dnia. Agent musi rowniez posiadac zdolnosc szybkiego finalizowania transakcji.
> Nasza firma oferuje pracownikom satysfakcjonujace wynagrodzenie oraz zabezpieczenie spoleczne.
>
> Jesli jestescie Panstwo zainteresowani podjeciem pracy na tym stanowisku, prosimy o wyslanie krotkiego CV na nasz adres e-mail:magellan.petroleum@gmx.com
>
> Nasz menedzer skontaktuje sie z Panstwem.

W polu "From:" ("Od:") znajdowało się wiele różnych adresów, wszystkie oczywiście podrobione. Kontakt z przestępcami nawiązywało się poprzez odpowiedź na adres znajdujący się w treści wiadomości. Zanotowaliśmy pięć adresów email, wskazanych do wysyłania CV:

```
m.petroleum@secretary.net
magellan.cv@europe.com
magellan.petroleum@gmx.com
magellan.petroleum@yahoo.com
magellan.resume@juno.com
```

Po nawiązaniu kontaktu z przestępcami, ofiara otrzymywała szczegółowy opis stanowiska pracy (5 stron – Rysunek 13, Rysunek 14) oraz formularz zgłoszeniowy (Rysunek 15), w którym należało podać bardzo szczegółowe dane osobowe. Wypełniony formularz należało zeskanować i przesłać na podany adres email.

AGENT DZIAŁU OPŁAT

Magellan

Obecna dostępność:TAK
Rodzaj zatrudnienia:Na pół etatu

WYMAGANIA OD KADYDATA

- minimum 18 lat
- dostęp do Internetu, aby szybko odpowiedzieć na e-maile,
- dostępność pod numerem telefonu (1-2 godziny dziennie),
- konto bankowe, aby przetwarzać opłaty,
- dobra historia kredytowa we własnym banku (możliwa jest opcja otworzenia konta bankowego),
- absolutny brak popełnionych przestępstw karnych lub wyroków,
- mile widziane doświadczenie w sprawach finansowych

Rysunek 13. Opis stanowiska pracy - wymagania

OBOWIĄZKI

Poszukujemy osób do zajmowania się wpłatami, pochodzącymi od naszych klientów. Magellan Petroleum Corporation dostępni agentowi szczegółowych instrukcji dotyczących operacji

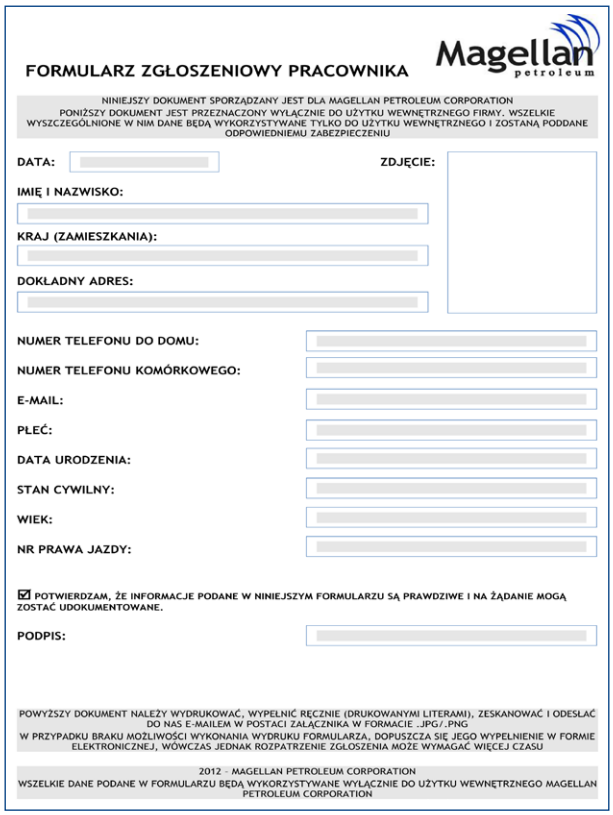
przetwarzania wpłat, łącznie z imieniem i nazwiskiem nadawcy oraz kwotą dla każdego przypadku.Po otrzymaniu wpłaty na konto bankowe pracownika obowiązkiem Agenta Finansowego jest wypłacenia gotówki i przelanie jej za pomocą Międzynarodowego Polecenia Przelewu lub za

pośrednictwem systemu przelewu pieniędzy International Western Union/Money Gram.Główna zaletą naszych usług jest najkrótszy możliwy czas, w którym sprzedawca otrzymuje pieniądze za sprzedane usługi/towary. Jeśli operacja jest opóźniona, nasz klient ma prawo anulowanie umowy, a my poniesiemy straty finansowe. Dlatego idealny kandydat musi być bardzo odpowiedzialny i ostrożny!

Rysunek 14. Opis stanowiska pracy - zakres obowiązków

W niektórych przypadkach następowała dodatkowa weryfikacja ofiary, polegająca na prośbie o podanie np. numeru telefonu oraz adresu zamieszkania członka rodziny bądź przesłania zeskanowanej kopii paszportu lub innego dokumentu tożsamości. W opisie stanowiska zawarte były informacje m.in. o prognozowanym wynagrodzeniu wraz z wyszczególnieniem składowych oraz zakres obowiązków. Można tam było również znaleźć sekcję „Pytania i Odpowiedzi", w której znajdowały się przejrzyście wytłumaczone zasady pobierania pieniędzy z konta oraz wykonanie polecenia przelewu z wykorzystaniem firmy Western Union lub MoneyGram.

Kiedy ofiara pomyślnie przeszła ten etap „rekrutacji", otrzymywała do podpisu rozbudowaną (ośmiostronicową) „Umowę na okres próbny" (Rys. 4). W ostatnim etapie „rekrutacji" należało oprócz podpisanej umowy wysłać zeskanowany obraz swojego prawa jazdy lub paszportu.



FORMULARZ ZGŁOSZENIOWY PRACOWNIKA

Magellan petroleum

NINIEJSZY DOKUMENT SPORZĄDZANY JEST DLA MAGELLAN PETROLEUM CORPORATION
PONIŻSZY DOKUMENT JEST PRZEZNACZONY WYŁĄCZNIE DO UŻYTKU WEWNĘTRZNEGO FIRMY. WSZELKIE WYSZCZEGÓLNIONE W NIM DANE BĘDĄ WYKORZYSTYWANE TYLKO DO UŻYTKU WEWNĘTRZNEGO I ZOSTANĄ PODDANE ODPOWIEDNIEMU ZABEZPIECZENIU

DATA:

ZDJĘCIE:

IMIĘ I NAZWISKO:

KRAJ (ZAMIESZKANIA):

DOKŁADNY ADRES:

NUMER TELEFONU DO DOMU:

NUMER TELEFONU KOMÓRKOWEGO:

E-MAIL:

PŁEĆ:

DATA URODZENIA:

STAN CYWILNY:

WIEK:

NR PRAWA JAZDY:

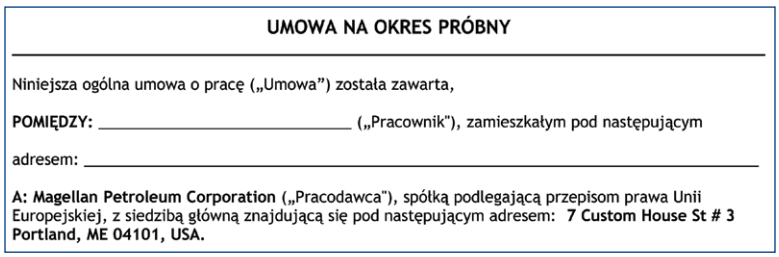
☑ POTWIERDZAM, ŻE INFORMACJE PODANE W NINIEJSZYM FORMULARZU SĄ PRAWDZIWE I NA ŻĄDANIE MOGĄ ZOSTAĆ UDOKUMENTOWANE.

PODPIS:

POWYŻSZY DOKUMENT NALEŻY WYDRUKOWAĆ, WYPEŁNIĆ RĘCZNIE (DRUKOWANYMI LITERAMI), ZESKANOWAĆ I ODESŁAĆ DO NAS E-MAILEM W POSTACI ZAŁĄCZNIKA W FORMACIE .JPG/.PNG
W PRZYPADKU BRAKU MOŻLIWOŚCI WYKONANIA WYDRUKU FORMULARZA, DOPUSZCZA SIĘ JEGO WYPEŁNIENIE W FORMIE ELEKTRONICZNEJ, WÓWCZAS JEDNAK ROZPATRZENIE ZGŁOSZENIA MOŻE WYMAGAĆ WIĘCEJ CZASU

2012 - MAGELLAN PETROLEUM CORPORATION
WSZELKIE DANE PODANE W FORMULARZU BĘDĄ WYKORZYSTYWANE WYŁĄCZNIE DO UŻYTKU WEWNĘTRZNEGO MAGELLAN PETROLEUM CORPORATION

Rysunek 15. Formularz zgłoszeniowy pracownika



UMOWA NA OKRES PRÓBNY

Niniejsza ogólna umowa o pracę („Umowa") została zawarta,

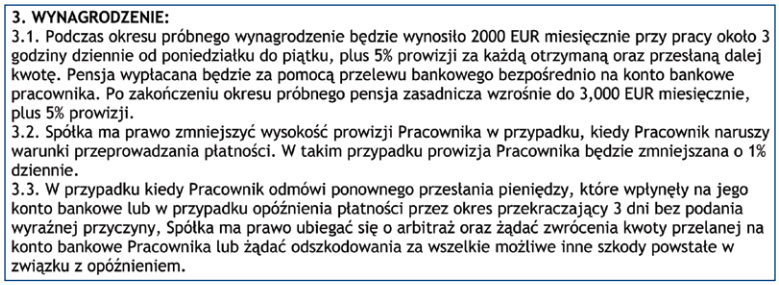
POMIĘDZY: _____ („Pracownik"), zamieszkałym pod następującym

adresem: _____

A: Magellan Petroleum Corporation („Pracodawca"), spółką podlegającą przepisom prawa Unii Europejskiej, z siedzibą główną znajdującą się pod następującym adresem: **7 Custom House St # 3 Portland, ME 04101, USA.**

Rysunek 16. Umowa

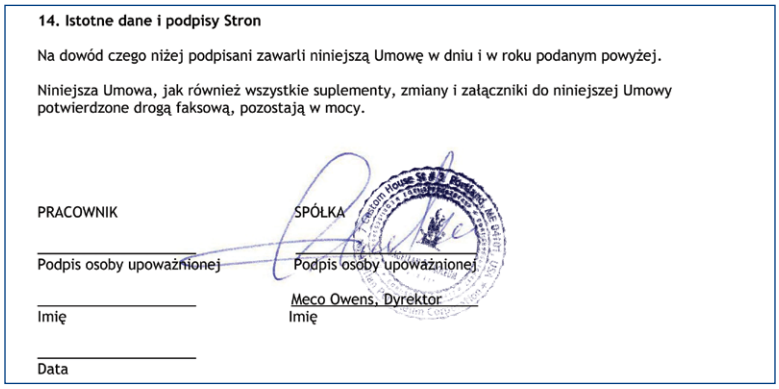
Umowa zawierała również szczegółowe zasady wynagradzania (Rys. 17).



3. WYNAGRODZENIE:
3.1. Podczas okresu próbnego wynagrodzenie będzie wynosiło 2000 EUR miesięcznie przy pracy około 3 godziny dziennie od poniedziałku do piątku, plus 5% prowizji za każdą otrzymaną oraz przesłaną dalej kwotę. Pensja wypłacana będzie za pomocą przelewu bankowego bezpośrednio na konto bankowe pracownika. Po zakończeniu okresu próbnego pensja zasadnicza wzrośnie do 3,000 EUR miesięcznie, plus 5% prowizji.
3.2. Spółka ma prawo zmniejszyć wysokość prowizji Pracownika w przypadku, kiedy Pracownik naruszy warunki przeprowadzania płatności. W takim przypadku prowizja Pracownika będzie zmniejszana o 1% dziennie.
3.3. W przypadku kiedy Pracownik odmówi ponownego przesłania pieniędzy, które wpłynęły na jego konto bankowe lub w przypadku opóźnienia płatności przez okres przekraczający 3 dni bez podania wyraźnej przyczyny, Spółka ma prawo ubiegać się o arbitraż oraz żądać zwrócenia kwoty przelanej na konto bankowe Pracownika lub żądać odszkodowania za wszelkie możliwe inne szkody powstałe w związku z opóźnieniem.

Rysunek 17. Zasady wynagradzania

Oczywiście umowa była podpisana przez „Dyrektora” i opatrzona pieczątką firmową (Rys. 18)



14. Istotne dane i podpisy Stron

Na dowód czego niżej podpisani zawarli niniejszą Umowę w dniu i w roku podanym powyżej.

Niniejsza Umowa, jak również wszystkie suplementy, zmiany i załączniki do niniejszej Umowy potwierdzone drogą faksową, pozostają w mocy.

PRACOWNIK

Podpis osoby upoważnionej

Imię

Data

SPÓŁKA

Podpis osoby upoważnionej

Meco Owens, Dyrektor

Imię

Rysunek 18. Fragment umowy zawierający podpis i pieczątkę

Jak zarobić 400 EUR za dwie godziny pracy

Kolejne kampanie zazwyczaj nie wykorzystywały wizerunku konkretnej firmy. Ich cechą charakterystyczną był prosty komunikat z ofertą pracy gwarantującą wysokie wynagrodzenie przy małym nakładzie pracy,

```
Poszukujemy współpracowników, którzy gotowi są podjąć się dodatkowej pracy.
Praca zajmie 1-2 godziny w tygodniu i nie wymaga żadnego wkładu pieniężnego.
Istotą pracy jest przetwarzanie napływających z Twojego miasta zamówień.

Jest to prosta praca, której można nauczyć się w ciągu 10 minut i będzie można regularnie
wykonywać ją dla naszej firmy.
Za każde przetworzone zamówienie otrzymasz od 200 do 500 EUR

Opłata – natychmiastowa!

Jeśli tylko zechcesz – będziesz mógł stale zwiększać ilość przetwarzanych zamówień.
Niestety my nie możemy zagwarantować zatrudnienia dla wszystkich chętnych,
dlatego proponujemy od razu wysłać nam swoje zgłoszenie.

Zwiększy to Twoją szansę, aby zostać członkiem naszego zespołu.

Co należy podać w zgłoszeniu:

Imię i nazwisko:
Adres e-mail:
Miasto, w którym mieszkasz:

Wniosek należy wysłać na nasz adres e-mail: xxx@xxx.com
Odpowiedź otrzymasz w ciągu dwóch dni roboczych.
```

Przykładowa wiadomości

W zależności od kampanii rozsyłane były wiadomości o zbliżonej treści, różne, ale podobnie wyglądające. Temat maila zachęcał do otwarcia wiadomości:

```
Czy dysponujesz dwoma wolnymi godzinami w tygodniu? Oto jak zarobc 185
EUR w tym czasie.
Poszukujemy w Twoim regionie pomocnikow do dobrze oplacanej pracy.

Poszukujemy zdalnych pracownikow do pracy na akord z wynagrodzeniem 95
EUR za 1 godzine.

Brakuje Ci pieniedzy? Proponujemy proste rozwiazanie. dodatkowa praca.

Zapraszamy do podjecia w wolnym czasie dodatkowej pracy z wynagrodze-
niem 95 EUR za 1 godzine.

Zarob 200-400 EUR za dwie godziny pracy juz w nastepnym tygodniu.
```

Przykładowa tematy wiadomośći

W tym wypadku również odpowiedź należało wysłać na adres mailowy podany w treści wiadomości. Wykorzystane domeny były zarejestrowane od niedawna i w swojej nazwie nawiązywały do firm rekrutacyjnych oraz portali z ofertami pracy.

```
jobrapidopl.com
jobspilotpl.com
graftonpl.com
toppolandjobs.com
topeuropajobs.com - EN
toppolandjobs.com
fastpolandjob.com
fasteurojobs.com - EN
jobspolska.com
quintcareerseu.com - EN
warszawaitpl.com
eurojobbnet.com - EN
artjobseu.com - EN
justpolandjob.com
pracainteria.com
totaljobspl.com
pracamoneypl.com
pracakariera.com
jobpilotpoland.com
```

Przykłady domen, w których znajdowały się adresy, na jakie należało przesłać zgłoszenie.

W zależności od kampanii rozsyłane były wiadomości o zbliżonej treści, różne, ale podobnie wyglądające. Temat maila zachęcał do otwarcia wiadomości:

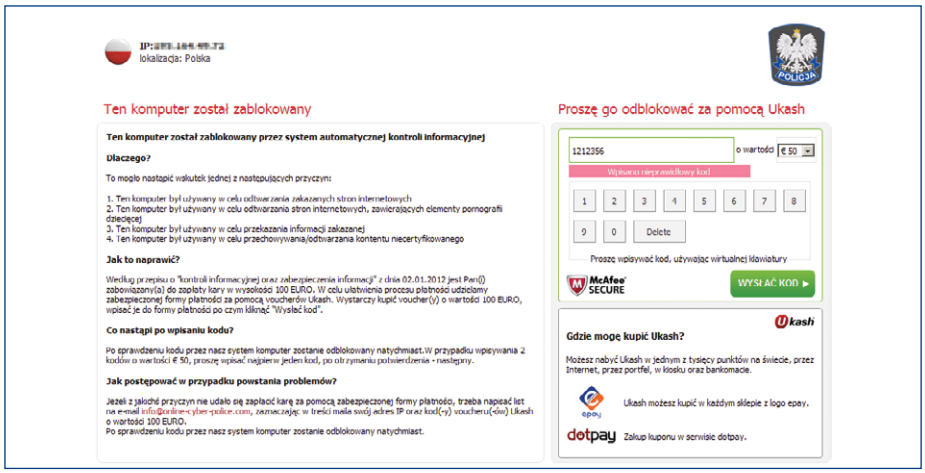
Podsumowanie

Opisane kampanie były skierowane do Polaków, o czym świadczy np. użycie poprawnej polszczyzny lub adresów mailowych nawiązujących w nazwach do polskich portali. Ogłoszenia pojawiały się również w uczelnianych biurach karier czy też na portalach zawierających oferty pracy. Kampanie mogły zatem zainteresować wiele osób, które w porę nie zorientowały się o podejrzanym charakterze „pracy".

4.3 Ransomware – Twój komputer został zablokowany!

Od maja 2012 roku obserwujemy aktywność złośliwego oprogramowania Weelsof oraz podobnych, stosujących dość przebiegłą socjotechnikę w celu wyłudzenia pieniędzy od użytkownika. Po zarażeniu systemu Veelsofem, dostęp do komputera jest blokowany z żądaniem zapłacenia „kary" w zamian za usunięcie blokady. Opłata wynosi 100 euro i powinna zostać dokonana poprzez podanie numeru vouchera UKASH. Przestępcy w zamieszczonym komunikacie powołują się na nieistniejące przepisy o „kontroli informacyjnej oraz zabezpieczenia informacji" z 2012 roku. Informacja napisana jest poprawną polszczyzną i dodatkowo – aby uwiarygodnić przekaz - opatrzona logiem policji!

Opisane działanie charakteryzuje rodzaj złośliwego oprogramowania zwany ransomware, który blokuje pewne funkcje komputera (np: szyfruje pliki, blokuje możliwość uruchomienia programów itp), a następnie za usunięcie blokady żąda wpłacenia okupu. Po zapłaceniu użytkownik dostaje zazwyczaj klucz/kod odblokowujący. Kwota okupu jest na ogół stosunkowo nieduża, co sprzyja wybraniu przez użytkownika takiej właśnie metody usunięcia problemu.



Rysunek19. Oprogramowanie Weelsof

Weelsof instaluje się metodą drive-by-download, a więc przez wejście na stronę z tzw. "exploit-packiem", który poprzez lukę w niezaktualizowanym oprogramowaniu przejmuje kontrolę nad systemem ofiary i ściąga z sieci oraz uruchamia złośliwe oprogramowanie. Po uruchomieniu ransomware dodaje parę wpisów do rejestru systemowego, wyłącza Eksplorator Procesów (znika menu 'start'), ukrywa wszystkie okna, a następnie wyświetla komunikat proszący o wniesienie opłaty. Z przeprowadzonej w laboratorium CERT Polska analizy wynika, iż malware nie podejmuje żadnych innych działań (tzn. nie infekuje/kasuje/szyfruje innych plików).

Analizy trojana Weelsof i sposoby usunięcia niektórych wariantów przedstawiliśmy na naszej stronie: **http://www.cert.pl/news/5483** oraz **http://www.cert.pl/news/5707**.

W przypadku natrafienia na problem związany z oprogramowaniem typu ransomware zalecamy zachowanie spokoju i kontakt z policją oraz serwisem komputerowym. Nie zalecamy natomiast wpłacania okupu. Problem nie dotyczy tylko Polski. Podobne przypadki ransomware pojawiły się w podobnym czasie na całym świecie, przy czym nierzadko jedno oprogramowanie miało zaszyte rozmaite komunikaty w wielu

językach, aktywowane w zależności od wersji językowej systemu. W kilku przypadkach operatorzy systemów płatności wykorzystywanych do wpłaty okupu zdecydowali się zamieścić na kuponach w punktach sprzedaży ostrzeżenie przed wykorzystywaniem ich do takich opłat.

4.4 Wyrafinowane ataki spyware na klientów bankowości internetowej – ZeuS Citadel, ZeuS P2P

Na początku września 2012 roku zauważyliśmy pojawiające się w plikach konfiguracyjnych oprogramowania szpiegowskiego wpisy, dotyczące systemów transakcyjnych polskich banków. Oprogramowanie atakowało komputery użytkowników systemu Windows. Po zainstalowaniu podsłuchiwało wszystkie przesyłane informacje (w tym głównie loginy i hasła) oraz, jeżeli posiadało dodatkowe instrukcje w pliku konfiguracyjnym, dokonywało podmiany treści wybranych stron internetowych tuż przed ich wyświetleniem. Tym złośliwym oprogramowaniem okazały się najnowsze odmiany ZeuSa: Citadel oraz ZeuS P2P (malware oparty na kodzie ZeuS 2.0.8.9, który wyciekł wiosną 2011 roku).

Na jakie ataki jest narażony użytkownik bankowości elektronicznej?

Celem ataków byli użytkownicy. To ich komputery były infekowane i podsłuchiwane przez atakujących. Od początku września w plikach konfiguracyjnych zaobserwowaliśmy wpisy dotyczące aż 15 różnych systemów transakcyjnych.

Zainfekowanie komputera umożliwia modyfikację treści strony banku. Atakujący może wyświetlić na monitorze dowolny komunikat. Sposób ataku i treść komunikatów ograniczone są jedynie przez inwencję twórczą przestępców, którzy cały czas mają pełną kontrolę nad komputerem. To świetny przykład połączenia metod socjotechniki oraz możliwości dostępu do zainfekowanego systemu. Użytkownik będzie przeświadczony, że czytane przez niego komunikaty pochodzą od banku. Pojawiły się przecież po zalogowaniu na konto i ponadto są podpisane przez “dział bezpieczeństwa Twojego Banku”! Ponieważ zmiany dokonywane są dopiero na etapie prezentacji treści użytkownikowi podczas ich wyświetlania w przeglądarce, nie wpływają one również w żaden sposób na alarmy związane z zabezpieczeniem transmisji szyfrowaniem SSL.

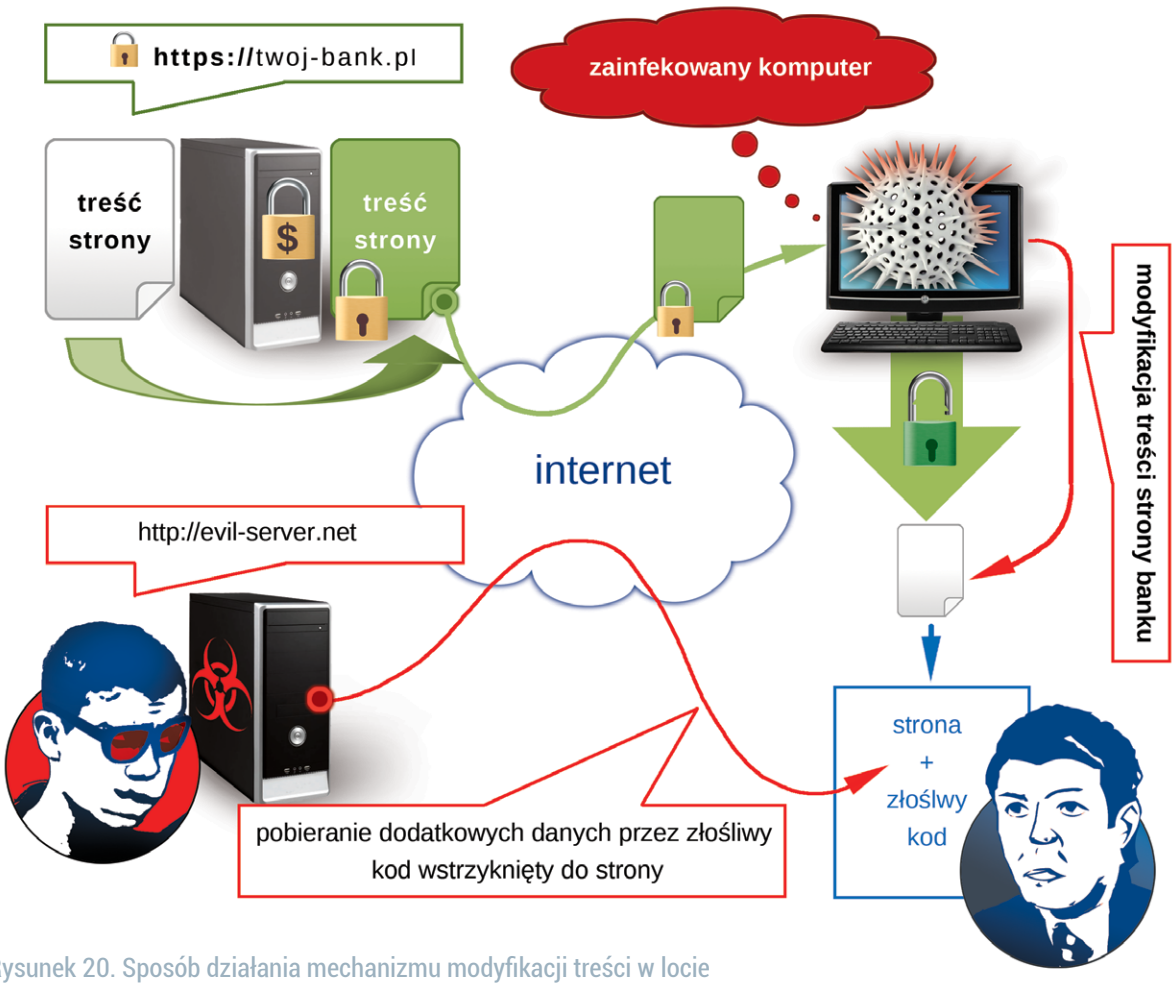
Poniżej przedstawiamy zestawienie zaobserwowanych dotychczas skutków zmian dokonywanych przez złośliwe oprogramowanie:

- Podmiana numeru konta docelowego oraz kwoty tuż przed zatwierdzeniem przelewu
- Podmiana aktualnego stanu konta
- Modyfikacja danych na liście wykonywanych operacji
- Okno proszące o podanie kodów jednorazowych w celu aktywacji/sprawdzenia funkcji bezpieczeństwa
- Okno proszące o podanie numeru telefonu oraz wybraniu modelu aparatu (atak ZitMo/2011)
- Monit proszący o zwrot środków pochodzących z błędnego/podejrzanego przelewu
- Monit proszący o wykonanie testowego przelewu w ramach aktywacji/sprawdzenia nowych funkcji bezpieczeństwa

Co tak naprawdę dzieje się w komputerze?

Po zainfekowaniu komputera użytkownik praktycznie przestaje być jego właścicielem. Już od dawna złośliwe oprogramowanie posiada możliwość podmieniania treści stron wyświetlanych na skażonym komputerze. Nie ma znaczenia czy połączenie było szyfrowane (https, kłódeczka przy adresie), ponieważ wprowadzenie zmian odbywa się już po odszyfrowaniu danych. Użytkownik nie ma żadnej możliwości weryfikacji, czy oglądana przez niego strona nie została zmodyfikowana przed wyświetleniem. Wprowadzane zmiany mogą być różne: od prostej zmiany jednego słowa – aż po doklejenie potężnych skryptów zawierających 3 000 linii kodu.

Rysunek 20 przedstawia sposób działania mechanizmu modyfikacji treści w momencie przeglądania strony. Informacja jest przygotowywana w systemie bankowym, a następnie przesyłana szyfrowanym (zielonym) kanałem do komputera użytkownika. Tutaj, w celu umożliwienia chociażby wyświetlenia, następuje odszyfrowanie treści. Jeżeli złośliwe oprogramowanie posiada w swojej konfiguracji wpisy dotyczące danej strony banku, następuje uruchomienie mechanizmu przechwytującego odszyfrowaną treść. Następnie wprowadzane są w niej zaprogramowane wcześniej zmiany. W niektórych przypadkach zmiany te mogą prowadzić do umieszczenia w stronie systemu bankowego elementów, które są pobierane (czerwony kanał) z serwera złodzieja. Nieświadomy zagrożenia użytkownik cały czas bez widocznych przeszkód korzysta z bankowości elektronicznej.



Rysunek 20. Sposób działania mechanizmu modyfikacji treści w locie

Jak uchronić się przed atakami?

Jedyną skuteczną metodą obrony przed atakami jest zachowanie czujności. Nowe i nieznane wcześniej komunikaty pojawiające się na stronie bankowości elektronicznej powinny być zawsze zgłaszane lub konsultowane z obsługą banku, nawet jeśli nie wydają się podejrzane. Wykorzystanie drugiego kanału, takiego jak rozmowa telefoniczna czy wizyta w placówce banku, pozwala zweryfikować czy odczytany komunikat naprawdę pochodził od naszego usługodawcy. Ponadto warto zaznaczyć, że banki rzadko (jeżeli w ogóle) wprowadzają w systemach zmiany bez uprzedniej szeroko zakrojonej akcji informacyjnej.

4.5 ZeuS P2P oraz ataki na jego sieć

ZeuS P2P nie jest pierwszym złośliwym oprogramowaniem, które wykorzystuje własną sieć P2P do komunikacji. Niewątpliwie implementacja tego sposobu komunikacji znacznie utrudnia walkę z malware oraz pozwala botmasterowi dłużej pozostać w ukryciu.

Słabością sieci P2P jest możliwość jej inwigilacji, ponieważ teoretycznie komputer będący elementem sieci może połączyć się z dowolnym innym. Przeczesywanie (crawling) sieci w ten sposób pozwala zidentyfikować adresy IP należące do zainfekowanych maszyn.

Realne zagrożenie dla polskich internautów

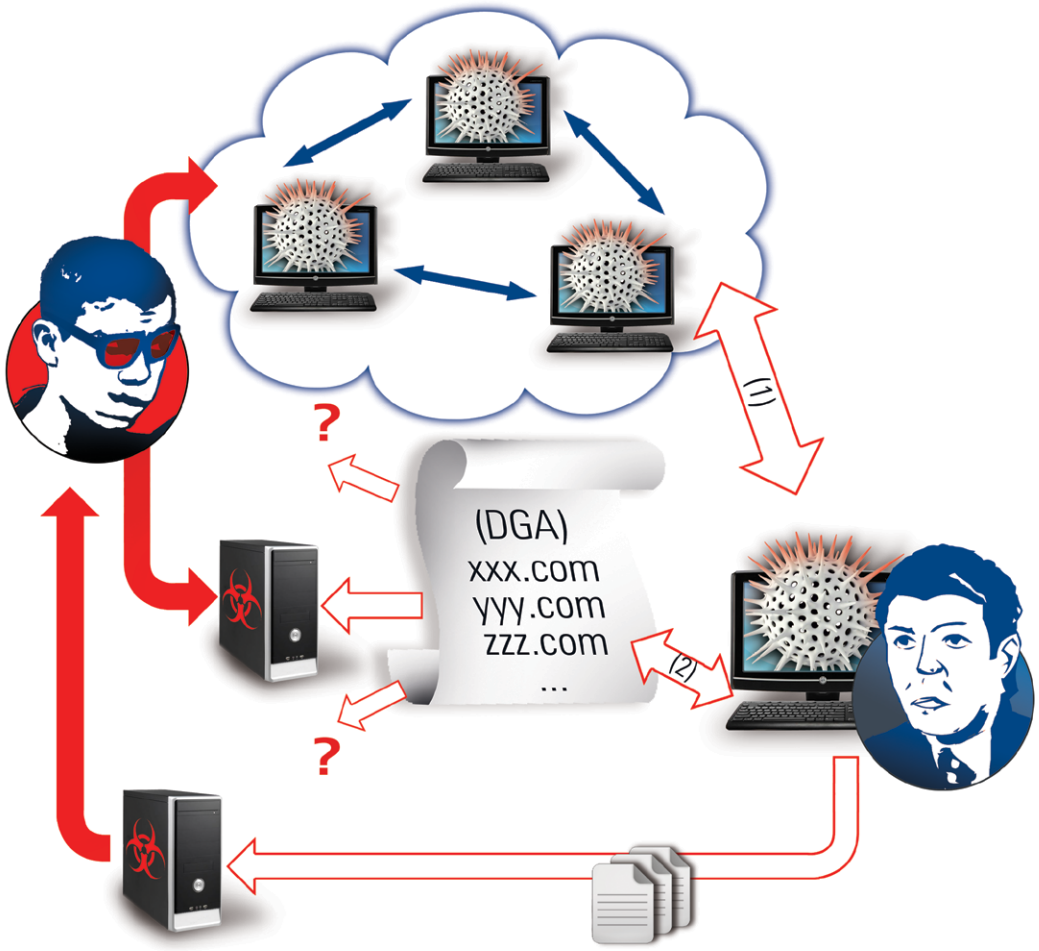
Od września do grudnia 2012 roku w plikach konfiguracyjnych ZeuSa P2P znajdowały się wpisy związane z adresami systemów transakcyjnych polskich banków. Bot posiadał reguły wstrzykiwania kodu aż dla 10 różnych adresów systemów. 26 grudnia 2012 roku wpisy te zostały usunięte z pliku konfiguracyjnego - niemniej jednak atak aktywny przez 4 miesiące zebrał na pewno sporą liczbę ofiar.

Jak działa ZeuS P2P?

W obecnej wersji ZeuS P2P wykorzystuje nadal dwa kanały komunikacji. Pierwszy - podstawowy - to sieć P2P. Jest ona wykorzystywana zarówno do wymiany danych związanych z utrzymaniem działania sieci P2P, jak i do przesyłania plików konfiguracyjnych oraz raportów do CnC. Drugi - zapasowy kanał to DGA - mechanizm generowania nazw domenowych.

Zostaje on aktywowany w sytuacji wykrycia problemów z działaniem sieci P2P, np.: brak aktywnych węzłów w tablicy sąsiadów. Jego działanie polega na generowaniu listy nazw domenowych kończących się na .ru .biz .info .org .net .com. Lista ta zawiera 1 000 pozycji i aktualizowana jest co 7 dni. Po jej wygenerowaniu bot próbuje łączyć się za pomocą protokołu HTTP kolejno z każdą wygenerowaną nazwą. Jeżeli połączenie powiedzie się, z podanego adresu pobierana jest „świeża” lista węzłów sieci P2P, która dodawana jest do tablicy sąsiadów.

Na początku 2012 roku kod ZeuSa P2P został znacząco zaktualizowany. Przede wszystkim modernizacji uległ mechanizm przesyłania danych do serwera C&C. W początkowej wersji dane te przesyłane były do konkretnych, zdefiniowanych adresów. Po aktualizacji dane przesyłane są za pomocą wybranych superwęzłów (supernode) sieci P2P. Ustalenie docelowego miejsca bez inwigilacji węzłów sieci jest więc wręcz niemożliwe. Innowacja ta pociągnęła za sobą konieczność implementacji kolejnego mechanizmu - obsługi pakietów rozgłaszających adresy superwęzłów. W aktualizacji dodano również możliwość pobierania zasobów (przez zasób w sieci P2P rozumiemy plik konfiguracyjny lub plik binarny) za pomocą protokołu UDP (dotychczas było to możliwe tylko za pomocą TCP).



Działanie sieci P2P

Komunikaty przesyłane przez sieć P2P można podzielić na dwie grupy: komunikaty służące do utrzymania sieci P2P oraz komunikaty służące wymianie danych. Do tej pierwszej można zaliczyć trzy rodzaje pakietów:

- Wymiana informacji o sąsiadach - służy do wymieniania się między komputerami informacją o adresach innych aktywnych węzłów w sieci P2P.
- Wymiana informacji o wersjach zasobów
- Dystrybucja informacji o superwęzłach - rozgłaszanie informacji o adresach oraz identyfikatorach węzłów sieci P2P używanych do przesyłania danych

Spośród komunikatów wykorzystywanych do wymiany danych można wyróżnić:

- Pobieranie nowych zasobów (przez protokół TCP oraz UDP)
- Przesyłanie danych przez sieć proxy superwęzłów
- Wymuszenie zdalnej aktualizacji zasobów (PUSH)

Aktualizacja zasobów

Proces aktualizacji zasobów bota składa się z paru etapów. W pierwszej kolejności malware wybiera z tablicy sąsiadów jeden z węzłów. Następnie wysyła do niego zapytanie o wersję zasobów.
W odpowiedzi otrzymuje pakiet zawierający wersję pliku konfiguracyjnego, pliku binarnego oraz numer portu TCP. Jeżeli otrzymane numery wersji są wyższe od wersji posiadanych zasobów, bot przechodzi do trybu aktualizacji. Początkowo próbuje pobrać nowy zasób za pomocą protokołu TCP z wykorzystaniem otrzymanego wcześniej numeru portu. Po poprawnym zestawieniu sesji TCP pobierany jest cały zasób. Jeżeli połączenie nie powiedzie się, bot ponawia próbę za pomocą protokołu UDP. Ze względu na charakter i ograniczenia protokołu UDP, pobieranie zasobu przy jego użyciu polega na sekwencyjnym pobraniu fragmentów o wielości ok. 1 KB do momentu skompletowania danych.

Ataki na sieć P2P oraz DGA

Lista możliwych scenariuszy ataków na sieć P2P, które były badane przez CERT Polska.

Wykorzystanie domen z DGA

Atak polega na wygenerowaniu listy domen za pomocą algorytmu DGA, a następnie zarejestrowaniu wybranych z nich. Następnie uruchomieniu pod danymi adresami serwera HTTP i umieszczeniu tam spreparowanego pliku zawierającego fałszywą listę węzłów.

Obrona: Dane umieszczane pod wygenerowanymi adresami opatrzone są podpisem cyfrowym. Bot po pobraniu danych sprawdza czy znaleziona sygnatura jest prawidłowa.

Dystrybucja fałszywych zasobów w sieci P2P

Atak polega na udostępnianiu fałszywych zasobów w sieci P2P.

Obrona: Bot po pobraniu danych (przez TCP lub UDP) sprawdza, czy zasób zawiera podpis cyfrowy, oraz czy podpis ten jest prawidłowy. Uniemożliwia to dystrybucję niepodpisanych zasobów w sieci P2P.

Fałszowanie wersji zasobu

Atak polega na wysłaniu fałszywej (zawyżonej) odpowiedzi na zapytanie o wersję. W ten sposób malware przechodzi w tryb aktualizacji i zaczyna pobierać nowe zasobów.

Obrona: Aby pobieranie zasobu zakończyło się powodzeniem, niezbędne jest dystrybuowanie danych z poprawnym podpisem cyfrowym. Istnieje więc możliwość zawyżenia wartości numeru wersji w odpowiedzi na zapytanie, a następnie w procesie pobierania udostępnienie starych danych posiadających poprawny podpis. Niestety wymieniane zasoby posiadają dodatkowe pole z numerem wersji. Po pobraniu danych i zweryfikowaniu podpisu po raz kolejny sprawdzany jest numer wersji (tym razem numer zakodowany w zasobie). Taka fałszywa aktualizacja zostanie więc odrzucona pomimo poprawnego podpisu cyfrowego.

Zatruwanie sieci fałszywymi węzłami

Jest to najbardziej typowy atak na sieci P2P. Polega on na odpowiadaniu na zapytania o sąsiednie węzły specjalnie spreparowaną listą adresów. Lista taka zawiera adresy komputerów będących pod kontrolą osoby przeprowadzającej atak. Powoduje to, iż komputery w poszukiwaniu kolejnych sąsiadów będą coraz częściej kontaktować się z atakującym - co w końcowym efekcie spowoduje zapełnienie tablicy sąsiadów spreparowanymi adresami. Niezbędne w tym przypadku jest poznanie mechanizmu, który decyduje o tym, jakie adresy i w jakiej sytuacji zostaną dodane do lokalnej tablicy sąsiadów.

Obrona: Obrona przed atakami tego typu jest najtrudniejszym zadaniem postawionym przed botmasterem. Wymienianie się adresami sąsiadów jest jednym z podstawowych mechanizmów utrzymujących poprawne działanie sieci P2P. Tak więc jedynymi środkami obrony jest odpowiednie zaprogramowanie mechanizmu aktualizującego lokalną listę sąsiadów tak np.: aby odrzucał podejrzane wpisy lub zduplikowane adresy.

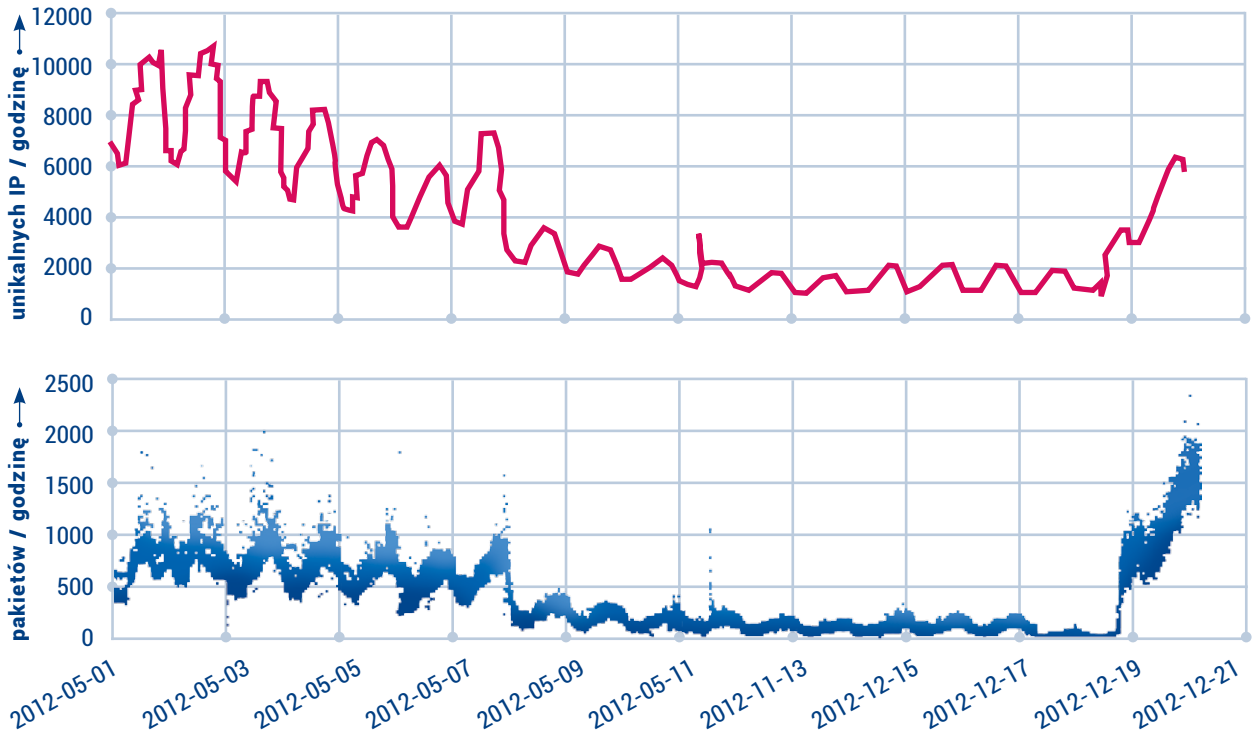
Zarejestrowane ataki na sieć P2P

Nasz system monitorowania sieci P2P w 2012 roku zarejestrował dwa prawie udane ataki. Prawie - ponieważ po niedługim czasie botnet był aktualizowany, co uodparniało go oraz przywracało kontrolę nad siecią P2P. Oba ataki polegały na zatruwaniu listy sąsiadów komputerów należących do botnetu.

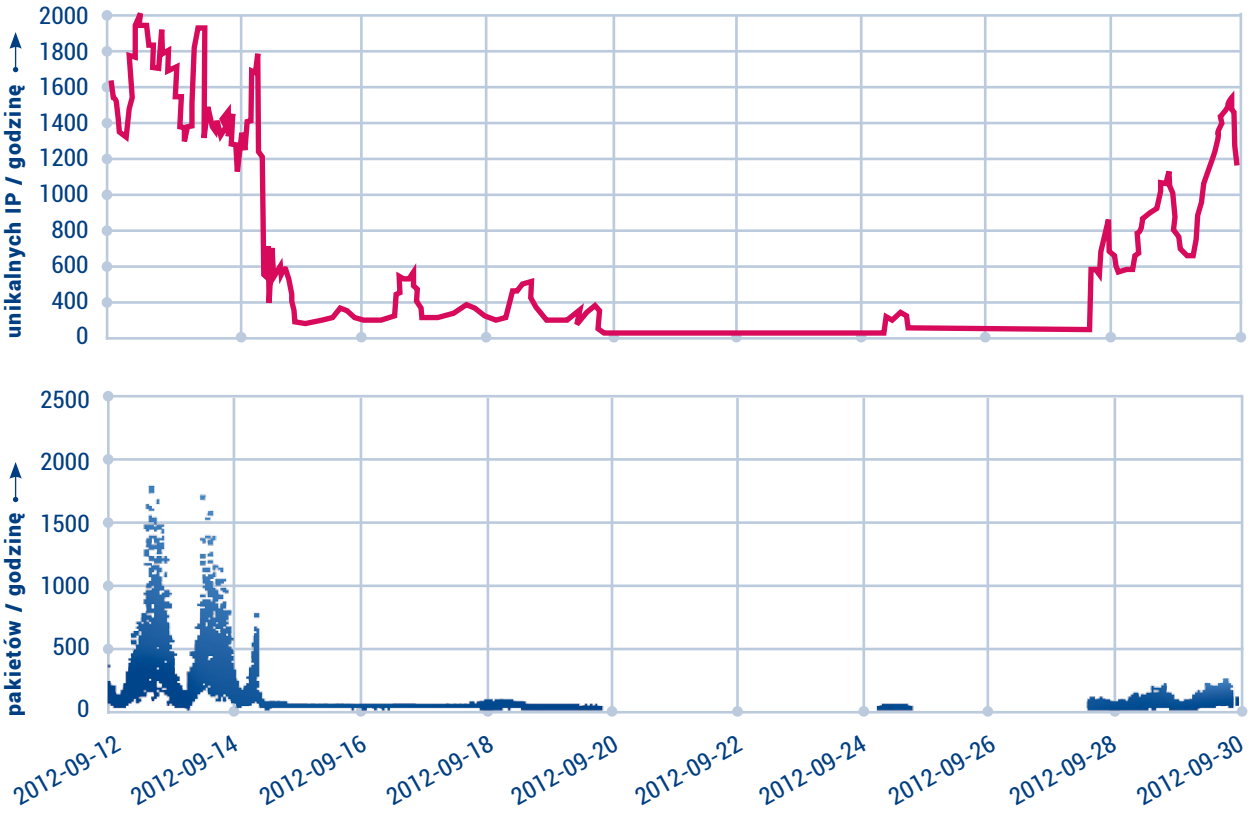
Przedstawiamy wykresy obrazujące aktywności w sieci P2P z punktu widzenia naszego systemu monitorowania. Jak widać, „Wiosenne zatruwanie" spowodowało powolny, lecz systematyczny spadek aktywności. Minimalna aktywność utrzymywała się aż przez 11 dni, po czym w sieci P2P została rozdystrybuowana nowa wersja bota. Spowodowało to zablokowanie ataku oraz gwałtowny wzrost rejestrowanej aktywności (rys.21, str.46).

Główną zmianą wprowadzoną w wiosennej aktualizacji było dodanie mechanizmu czarnej listy. Czarna lista jest zakodowana w pliku binarnym bota i zawiera 22 sieci IP. Jeżeli adres komputera łączącego się z botem należy do jednej z tych sieci, jego pakiety zostaną zignorowane.

„Jesienne zatruwanie" zadziałało znacznie szybciej. Atak spowodował szybki spadek aktywności - a po paru dniach wskazania systemu monitorowania sięgnęły prawie zera. Niemniej jednak po raz kolejny udało się wypuścić i rozdystrybuować aktualizację, która pozwoliła przywrócić sieć P2P do działania. Tym razem zajęło to 13 dni:



Rysunek 21. Aktywność w sieci P2P w systemach monitorowania CERT Polska – „Wiosenne zatruwanie"



Rysunek 22. Aktywność w sieci P2P w systemach monitorowania CERT Polska – „Jesienne zatruwanie"

Aktualizacja wprowadziła kolejne mechanizmy utrudniające zatruwanie sieci P2P fałszywymi sąsiadami. Pierwszy ogranicza występowanie na liście sąsiadów adresów należących do tej samej podsieci (255.255.255.0). Inny ogranicza ilość pakietów obieranych od jednego adresu IP do 10 na 60 sekund.

4.6 Flame

Flame (znany też jako: Flamer, Skywiper) jest skomplikowaną aplikacją typu koń trojański, odkrytą w 2012 roku. Od tego czasu jest przedmiotem obszernej analizy[1] prowadzonej przez ekspertów od złośliwego oprogramowania. Badacze Flame'a zwracają uwagę przede wszystkim na jego niezwykle skomplikowany kod, modułową konstrukcję i zaawansowane algorytmy, które wykorzystuje. Właśnie stopień skomplikowania tego trojana stał się przyczyną powstania wielu hipotez na temat jego pochodzenia[2]. Jedną z najwcześniejszych publikacji na temat Flame'a jest raport laboratorium CrySyS[3], który zawiera głównie obserwacje poczynione w trakcie analizy behawioralnej, takie jak: sposoby interakcji z systemem operacyjnym, systemem plików, siecią, parametrami czasowymi. Właśnie ten raport zainspirował nas do przyjrzenia się Flame'owi bliżej i odkrycia kilku jego wcześniej niepublikowanych aspektów.

---

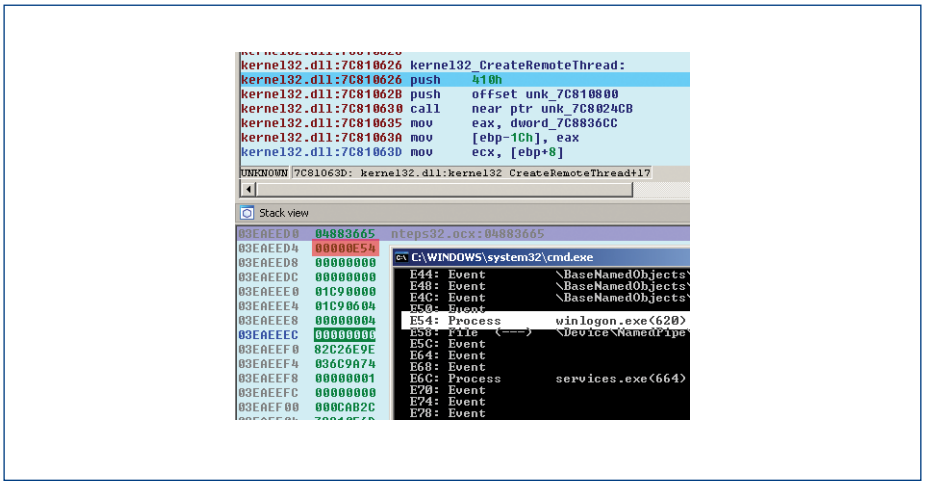
1 *http://www.securelist.com/en/blog/208193522/*
http://blog.eset.com/2012/07/20/flame-in-depth-code-analysis-of-mssecmgr-ocx

2 *http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html*

3 *http://www.crysys.hu/skywiper/skywiper.pdf*

4.6.1 Wstrzykiwanie kodu

Flame także wstrzykuje wątki w trakcie swojego procesu instalacji, ale w jego przypadku zwykłe wstrzykiwanie wątków zmieniono w precyzyjne narzędzie pozwalające na transfer własnego kodu do innych procesów i wątków. Jest ono intensywnie używane w ciągu całego cyklu życia Flame'a (od infekcji do samozniszczenia). Flame korzysta z tego narzędzia by przenosić i kopiować własne elementy w różne części systemu operacyjnego ofiary z zaskakującą sprawnością. W trakcie naszej analizy odkryliśmy ciekawą i rozbudowaną technikę wstrzykiwania wrażliwych części kodu.



Rysunek 23. wstrzykiwanie kodu za pomocą funkcji CreateRemoteThread

4.6.2 Łańcuch wstrzyknięć

Jak możemy przeczytać w raporcie laboratorium CrySyS:

"W trakcie startowania, mssecmgr.ocx jest ładowany jako pakiet uwierzytelniający LSA. Około 2 minuty później, services.exe ładuje moduł advnetcfg.ocx. Proces ten powtarza się co 2, 3 minuty, łącznie 3 razy. Około 2 minuty później, services.exe ładuje moduł nteps32.ocx z mssecmgr.ocx, następnie winlogon.exe również ładuje nteps32.ocx. Ten plik jest ładowany kilka razy. W międzyczasie, explorer.exe tworzy 5 procesów iexplore.exe, które tworzą plik wpgfilter.dat."

[CrySyS Skywiper report, Activation and propagation, Startup sequence, tłum. aut.]

Najbardziej interesującym fragmentem tego opisu wydał nam się proces explorer.exe, który nagle uruchamia kilka instancji procesu iexplore.exe. Wyjaśnijmy, co to oznacza: Flame dokonał propagacji swojego kodu przez cztery procesy, by rozpocząć wykonywanie swoich złośliwych funkcji! Zdecydowaliśmy się na dokładniejsze poznanie i zbadanie tego mechanizmu.

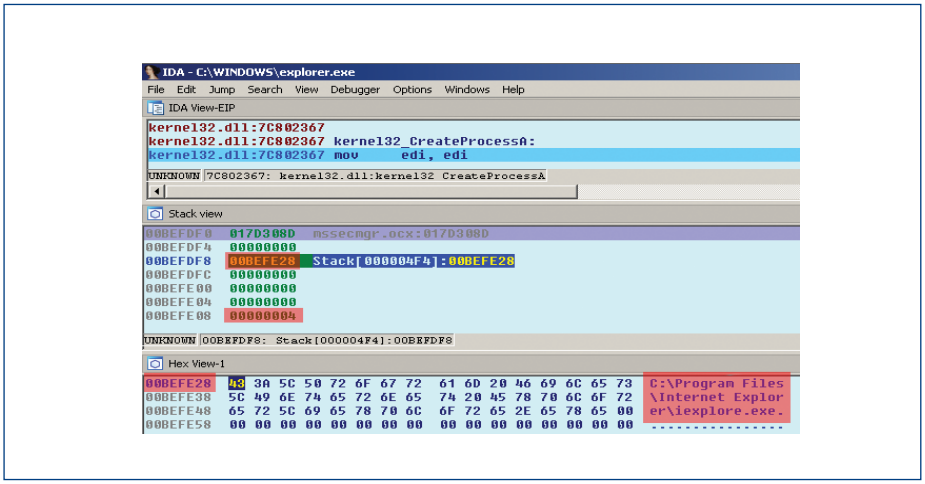
Rysunek 24. Propagacja kodu Flame

Proces wstrzykiwania

Komputer ofiary jest infekowany m.in. za pomocą wykorzystania luki MS10-061[4] . Po udanym włamaniu ładowany jest program rundll32.exe, który z kolei ładuje i rozpoczyna wykonywanie kodu głównego modułu Flame'a – mssecmgr.ocx. Wykonuje on różne operacje instalacyjne (między innymi rejestruje usługę LSA, dzięki której bot załaduje się w trakcie ładowania systemu operacyjnego po zrestartowaniu komputera), a następnie odnajduje proces services.exe i wstrzykuje do niego części swojego kodu.

Rysunek 25. Wstrzykiwanie kodu do explorer.exe

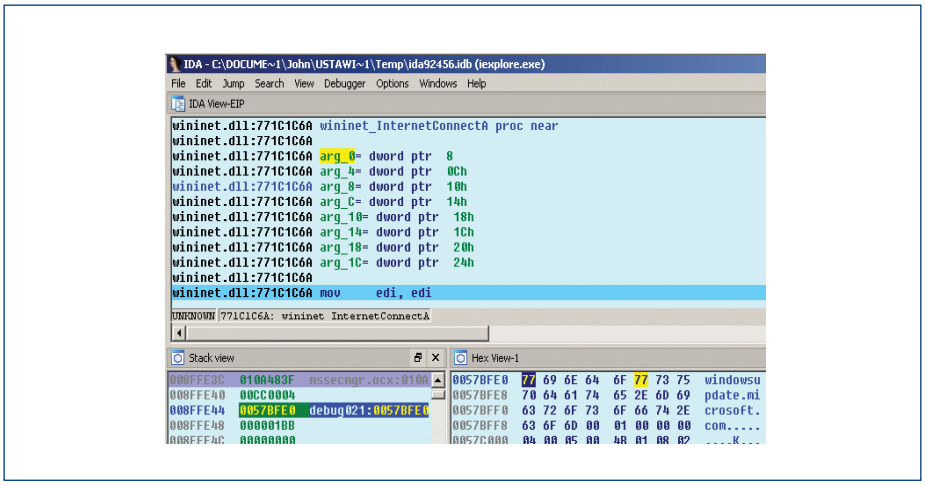
Następnie services.exe dystrybuuje za pomocą zwykłych wstrzyknięć kolejne części złośliwego kodu do różnych elementów systemu operacyjnego. Przygotowuje także i wstrzykuje kod do procesu explorer.exe. Podążyliśmy tropem tego wstrzyknięcia i rozpoczęliśmy analizę także tego procesu. Okazało się, że wstrzyknięty wątek oczekuje na sygnał wydany przez services.exe, a następnie uruchamia proces programu iexplore.exe z zatrzymanym wykonaniem głównego wątku.



Rysunek 26. Uruchomienie procesu iexplorer.exe

[4] *http://www.securelist.com/en/blog/208193522/*

Od tej chwili procesy services.exe i iexplore.exe komunikują się ze sobą za pośrednictwem potoku, nazwanego w naszym przypadku: **PipeGx16** (jednak możliwe, że nazwa ta została skonstruowana z częściowo wylosowanych znaków i inne instalacje będą dysponować innymi nazwami). Wątek działający w kontekście procesu services.exe zapisuje swoje rozkazy do tego potoku, a iexplore.exe odczytuje je i wykonuje. Jednym z zarejestrowanych przez nas rozkazów jest rozkaz nawiązania połączenia z adresem windowsupdate.microsoft.com, jak pokazano na ilustracjach. Jest to dowód na prowadzenie przez bota Flame złośliwych operacji – ustanawianie ukrytego połączenia. Działanie to może mieć na celu zbadanie, czy komputer ma działające połączenie z Internetem, jak również (co bardziej prawdopodobne) wstęp do tzw. ataku "Gadget"[5]. Proces iexplore.exe działa i wykonuje instrukcje, dopóki potok PipeGx16 nie zostanie zamknięty. Jeśli to się stanie, explorer.exe kończy jego działanie.



Rysunek 27. Inicjowanie połączenia z adresem windowsupdate.microsoft.com

4.6.3 Unikanie wykrycia

Omawiany proces jest najbardziej wyrafinowaną techniką wstrzykiwania kodu, jaką do tej pory zaobserwowaliśmy w złośliwym oprogramowaniu. Zazwyczaj proces wykonywania złośliwych funkcji (takich jak nawiązywanie ukrytych połączeń) był prostszy. Nawet zaawansowane trojany bankowe posługiwały się tylko jednym wstrzyknięciem wątku (złośliwy kod uruchamiany był w jednym procesie). Natomiast proces przeprowadzany przez Flame wykorzystuje aż trzy wstrzyknięcia. Jest to także jeden z dowodów na rozbudowany projekt architektoniczny tej aplikacji. Dlaczego warto przeprowadzać tę operację w aż tak skomplikowany sposób? Odpowiedź na to pytanie jest oczywista: aby pozostać niewykrytym przez możliwie długi czas. Przyjrzyjmy się zatem znamiennym cechom mechanizmów wstrzyknięć Flame'a.

Przede wszystkim ukryte połączenie z Internetem jest tworzone przez proces iexplore.exe. W ten sposób Flame unika wykrycia przez zautomatyzowane narzędzia i powierzchowną analizę. Na przykład, połączenie zestawiane przez proces explorer.exe (jak to ma miejsce w przypadku np. bota SpyEye czy ZeuS) jest podejrzaną oznaką, dlatego że wykonywanie tego typu połączeń nie leży w kompetencji tego procesu. Przeciwnie ma się sprawa z iexplore.exe, którego głównym zadaniem jest interakcja z siecią. Także próba połączenia z witryną Windows Update nie wzbudzi podejrzeń nawet w dokładnie

[5] *http://www.securelist.com/en/blog/208193558/Gadget_in_the_middle_Flame_malware_spreading_vector_identified/*

obserwowanych segmentach sieciowych korporacji i instytucji rządowych, ponieważ każdy spodziewa się, że systemy Windows będą tam aktualizowane. Poza tym sądzono, że aktualizacje są przecież chronione przez "bezpieczne" funkcje kryptograficzne. Niestety, Flame ma sposoby także i na przełamanie tych zabezpieczeń – wspomniany już atak Gadget. Jest to niezwykle wyrafinowany, bardzo trudny do wykrycia, atak wykorzystujący exploit typu 0day.

Fakt, że proces iexplore.exe jest rozpoczynany i kończony przez explorer.exe, sprawia, że operacje te wyglądają bardzo naturalnie. Zazwyczaj, kiedy użytkownik otwiera swoją ulubioną przeglądarkę, robi to właśnie za pomocą interfejsu explorer.exe. Dlatego Flame wykorzystuje ten proces jako swoiste proxy i pozostawia całą hierarchię procesów nietkniętą.

4.6.4 Podsumowanie

Flame wykorzystuje najbardziej zaawansowany mechanizm wstrzykiwania kodu, jaki do tej pory zaobserwowaliśmy w złośliwym oprogramowaniu. Dystrybuuje on swoje elementy wśród systemowych procesów wykorzystując łańcuchy do trzech wstrzyknięć i propaguje swój kod poprzez cztery procesy, by ostatecznie wykonać funkcje konia trojańskiego. Taka dystrybucja wśród różnych procesów, także z uwzględnieniem ich naturalnej hierarchii, znacznie utrudnia wykrycie za pomocą analizy behawioralnej. Ten system to jedna z wielu wyjątkowych cech Flame'a, które pozwoliły mu działać niewykrytym przez miesiące i lata.

4.7 Wykorzystywanie domen .pl

W 2012 roku zaobserwowaliśmy niepokojące zjawisko coraz częstszego wykorzystywania nazw domenowych z końcówką .pl do zarządzania złośliwym oprogramowaniem i botnetami, a także innych działań przestępczych (np. utrzymywanie stron do handlu nielegalnymi farmaceutykami).

Przestępcy często odwołują się do kontrolerów C&C za pośrednictwem nazw domenowych (a nie bezpośrednio przez numer IP), co pozwala im na większą elastyczność w zarządzaniu infrastrukturą – mogą m.in. łatwiej przenosić serwery do innych dostawców, a także stosować mechanizmy typu fast-flux. Choć usunięcie problematycznej domeny z rejestru jest rzeczą prostą z technicznego punktu widzenia, często wiąże się z wątpliwościami natury prawnej. Z tej słabości skrupulatnie korzystają przestępcy, którzy zamiast korzystać z bezpłatnych domen drugiego i wyższych rzędów, wykupują je w domenach narodowych różnych państw, w tym Polski. W pojedynczym przypadku (atak RunForestRun, masowo kompromitujący strony wykorzystujące Plesk Panel) wykorzystano algorytm DGA (Domain Generation Algorithm) do tworzenia unikalnych nazw w domenie z końcówką .waw.pl. Wcześniej w tym samym ataku używano adresów w domenie .ru.

W Tabel 21 zestawione zostały boty łączące się z domenami .pl, według liczby nazw domenowych. W przypadku większości z nich domeny rozwiązywały się na adresy IP znajdujące się za granicą, przede wszystkim w Chinach, Rosji czy na Łotwie.

Virut	43
ZeuS/Citadel	28
Dorkbot	4
SpyEye	4
Inne	39

Tabela 21. Najczęściej obserwowane botnety wykorzystujące domeny.pl (według liczby domen)

5 Najciekawsze wydarzenia z działalności CERT Polska

5.1 Konferencja SECURE 2012

Międzynarodowa konferencja na temat bezpieczeństwa teleinformatycznego SECURE, organizowana w dniach 22-24 października 2012 roku przez instytut badawczy NASK i działający w jego strukturach zespół CERT Polska, odbyła się już po raz szesnasty. Tegoroczna edycja zgromadziła w warszawskim Centrum Nauki Kopernik rekordową liczbę 46 prelegentów zajmujących się zagrożeniami sieciowymi oraz ponad 300 uczestników z Polski i ze świata.

Wśród zagranicznych ekspertów, obecnych na SECURE 2012, byli m.in. dr Jose Nazario z The Honeynet Project, który opowiedział o sposobach tropienia sieci botnetowych, Chris Novak z Verizon, który ze współprelegentami przedstawił przypadki wycieków danych z dużych firm oraz dostępne metody zaradcze, oraz Robert McArdle z Trend Micro, który przybliżył wartość internetowej tożsamości użytkownika i słabości HTML5. Ciekawym aspektem konferencji był również pierwszy w Polsce występ prelegenta z Twittera, Aleksandra Kołcza. Na uwagę zasługiwała również obecność Rika Fergusona z Trend Micro, jednego z czołowych ekspertów bezpieczeństwa informatycznego doradzającego m.in. rządowi brytyjskiemu oraz Ryana Pittmana, który przybliżył działalność NASA w zakresie zwalczania cyberprzestępczości.

SECURE 2012 była również szansą do zapoznania się z dorobkiem rodzimych ekspertów zajmujących się cyberbezpieczeństwem. Piotr Konieczny, założyciel serwisu niebezpiecznik.pl, opowiadał, jakie informacje o użytkownikach można znaleźć w sieci oraz jak mogą być wykorzystane przeciw nim.

Z kolei Błażej Szymczak z Allegro przedstawił ludzkie słabości wykorzystywane w świecie e-handlu. Szczególnym zainteresowaniem cieszyły się również wystąpienia przedstawicieli NASK i CERT Polska. Paweł Pawliński z CERT Polska przedstawił kliencki system honeypotów Honey Spider Network 2.0. Po jego wystąpieniu uczestnicy konferencji mieli możliwość przetestowania publicznej części serwisu jeszcze przed oficjalną premierą. Tomasz Bukowski i Radosław Żuber przedstawili natomiast przekrój najciekawszych zgłoszeń incydentów z ostatniego roku pracy zespołu CERT Polska. Z kolei Anna Rywczyńska, koordynatorka projektu Safer Internet w Polsce, przybliżyła zgromadzonym projekt „Zostań znajomym swojego dziecka".

W dniach 22 i 25 października odbyły się również warsztaty SECURE Hands-on. Pięć spotkań, w tym dwa prowadzone również przez ekspertów z CERT Polska, zgromadziło 88 uczestników. Ich tematyka dotyczyła m.in. praktycznych metod wykrywania ataków w sieci oraz zagrożeń dla klientów bankowości elektronicznej.

Konferencję patronatem medialnym objęły redakcje: PAP Nauka w Polsce, Gazeta Technologie, Niebezpiecznik.pl, eGospodarka, Bank, Business Security Magazine, IT Professional, IT w Administracji, Zaufana Trzecia Strona.

Partnerami SECURE 2012 były firmy: Chartis Europe Oddział w Polsce, Dr. WEB, EmiTel, EURid, HP, Integrated Solutions, PaloAlto, RSA, Symantec, Systemics PAB, Qualis, Matic, Websense.

5.2 NISHA

Z początkiem 2012 roku CERT Polska rozpoczął prace nad zaplanowanym na lata 2012-2014 projektem NISHA (Network for Information Sharing and Alerting). Jego celem jest wzrost świadomości użytkowników w kwestii bezpieczeństwa on-line poprzez rozwinięcie istniejącego prototypu systemu ostrzegania i wymiany informacji o bezpieczeństwie. Prototyp został stworzony w ramach prac przy wcześniejszym projekcie FISHA, prowadzonym w latach 2009-2011. NISHA ma natomiast zaowocować pilotażową siecią złożoną z czterech głównych węzłów-portali, które będą działać w każdej z instytucji biorących udział w projekcie i aktywnie wymieniać między sobą informacje o bezpieczeństwie oraz udostępniać je lokalnie w swoich językach narodowych. W następnej kolejności sieć będzie rozbudowywana o portale partnerów zainteresowanych otrzymywaniem lub/i dodawaniem informacji do sieci NISHA.

Każdy z węzłów, poza wymianą danych między sobą, ma na celu dotarcie z informacjami krążącymi w sieci NISHA do użytkowników domowych oraz kadry pracowniczej sektora małych i średnich przedsiębiorstw. Skupienie się na tych grupach wynika z faktu, że poprzez swoją liczebność odgrywają kluczową rolę w bezpieczeństwie Internetu, będąc jednocześnie łatwym celem ataków z powodu niskiej znajomości zagadnień bezpieczeństwa. Każdy z partnerów, w oparciu o przygotowane w ramach projektu rozwiązania techniczne oraz prawne, zadba o utrzymanie sieci i dotarcie z informacją do grup docelowych poprzez odpowiednich brokerów informacji (portale informacyjne, radio, telewizja) w swoim kraju. Proste mechanizmy udostępniania informacji w systemie umożliwią krajowym serwisom informacyjnym, które nie są członkami sieci NISHA, łatwe wykorzystanie informacji bez konieczności nadmiernych nakładów prac technicznych. Idea zaangażowania brokerów informacji ma pomóc zmniejszyć lukę w komunikacji między użytkownikami Internetu a specjalistami bezpieczeństwa.

W roku 2013, w ramach krajowych działań związanych z NISHA, będziemy aktywnie szukać partnerów wśród polskich portali internetowych i mediów, aby mogły one swobodnie korzystać z informacji zamieszczonych w portalu i dostarczać je swoim odbiorcom.

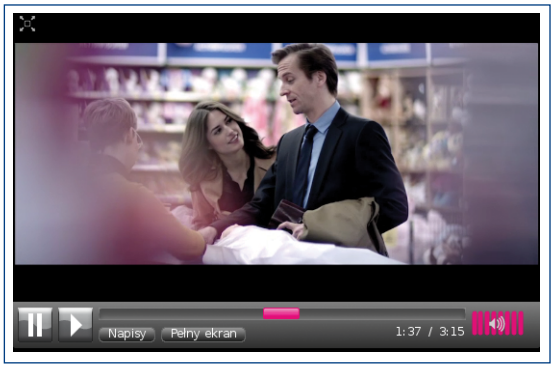
Projekt NISHA jest współfinansowany przez Komisję Europejską w ramach programu „The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks" (CIPS). W skład konsorcjum pracującego nad NISHA, oprócz CERT Polska (NASK), wchodzą narodowe zespoły CERT z Węgier (PTA/CERT Hungary) i Portugalii (FCCN/CERT.PT) oraz Institute for Internet Security (Institut für Internet-Sicherheit) z Westfälischen Hochschule w Gelsenkirchen.

Kod źródłowy stworzonego w ramach projektu oprogramowania będzie udostępniony na Licencji Publicznej Unii Europejskiej (EUPL) [6].

5.3 EISAS

Aby stale podnosić poziom świadomości bezpieczeństwa cybernetycznego obywateli i przedsiębiorstw w krajach Unii, Komisja Europejska zdecydowała się promować współpracę państw członkowskich w działaniach zmierzających do podnoszenia tej świadomości w Europie. W 2006 roku zainicjowała stworzenie EISAS, europejskiego systemu wymiany informacji dotyczących bezpieczeństwa komputerowego

[6] *http://joinup.ec.europa.eu/system/files/PL/EUPL%20v.1.1%20-%20Licencja.pdf*



Rysunek 28. Film "Bluff City"

oraz ostrzegania przed zagrożeniami w Internecie, który ma na celu wzmacnianie współpracy pomiędzy instytucjami bezpieczeństwa tak, aby skutecznie dotrzeć do użytkowników domowych oraz kadry małych i średnich przedsiębiorstw z istotnymi informacjami o bezpieczeństwie. Techniczną realizacją EISAS jest projekt NISHA (5.2).

W roku 2012 Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) przeprowadziła pilotaż EISAS, polegający na stworzeniu atrakcyjnych materiałów o bezpieczeństwie w kilku językach, a następnie rozpowszechnieniu ich przez organizacje w wybranych krajach członkowskich UE poprzez swoje kanały komunikacji. Zespół CERT Polska uczestniczył w opracowaniu wersji materiałów dla polskich użytkowników. Poza CERT Polska, projekt wsparły CERT-y z Niemiec, Norwegii, Węgier, Portugali i Hiszpanii dostosowując materiały do potrzeb i specyfiki każdego kraju oraz biorąc udział w ich promocji.

Tematyka przygotowanych w ramach projektu EISAS materiałów edukacyjnych objęła zagadnienia dotyczące najbardziej krytycznych zagrożeń dla przeciętnego użytkownika Internetu: **kradzieży tożsamości, inżynierii społecznej i botnetów**. Na każdy temat przygotowano napisane przystępnym językiem poradniki, dodatkowo uatrakcyjnione przez interaktywny test podatności na kradzież tożsamości oraz profesjonalnie nakręcony film „Bluff City" o zagrożeniach inżynierii społecznej. Linki do materiałów EISAS można znaleźć na naszym blogu **http://www.cert.pl/news/6193.**

Wnioski z przeprowadzonego pilotażu podkreśliły znaczenie współpracy publiczno-prywatnej w pozyskiwaniu dobrej jakości materiałów uświadamiających oraz na konieczność utrzymania schematu dystrybuowania takich informacji przez lokalnych pośredników. Naturalnym kandydatem na rozwiązanie wspomagające wymianę informacji w tej dziedzinie wskazano projekt NISHA.

5.4 Raport ENISA o honeypotach

22 listopada 2012 roku Europejska Agencja ds. Bezpieczeństwa Informacji – **ENISA** – opublikowała raport o zastosowaniu honeypotów do wykrywania zagrożeń sieciowych: „**Proactive Detection of Security Incidents: Honeypots**". Studium wykonane zostało przez zespół CERT Polska. Jest to pierwsze tak obszerne badanie tej technologii pod kątem jej użyteczności do pracy zespołów typu CERT i jednocześnie pierwszy na świecie tak szeroki przegląd dostępnych darmowych rozwiązań. W przeciwieństwie do poprzednich badań akademickich dotyczących honeypotów, staraliśmy się przyjąć bardzo praktyczne podejście do oceny istniejących rozwiązań typu honeypot.

Najogólniej ujmując, honeypot jest zasobem umieszczonym w sieci, którego jedynym zadaniem jest zostanie zaatakowanym, skompromitowanym, badanym lub wykorzystanym w inny nieautoryzowany sposób. Zasób może być praktycznie dowolnego charakteru: może być to serwis, aplikacja, system lub ich zestaw, albo też po prostu jakaś informacja. Podstawowym założeniem jest to, że każdy, kto próbuje się połączyć lub korzystać z takiego zasobu w jakikolwiek sposób, jest z definicji podejrzany. Cała interakcja pomiędzy honeypotem i podmiotem, który się z nim łączy jest monitorowana i analizowana w celu wykrycia i potwierdzenia złośliwych działań.

Honeypoty mogą być stosowane do wielu różnych celów na przykład do: monitorowania aktywności botnetów i robaków w sieci Internet, zbierania informacji o zainfekowanych komputerach w sieci,

identyfikacji nowych exploitów i podatności w systemach, wykrywania i zbierania złośliwego oprogramowania, badania zachowań hakerów, szukania wewnętrznych infekcji w sieci lub ataków wewnętrznych.

W naszych badaniach skupiliśmy się na ocenie i analizie istniejących, darmowych honeypotów. Aby osiągnąć ten cel opracowaliśmy nowe kryteria oceny honeypotów, skupiając się na praktyczności tych rozwiązań. Pobraliśmy i przetestowaliśmy 30 honeypotów typu „standalone" tzn. honeypotów, które można samemu zainstalować u siebie w sieci. Wyróżniliśmy szereg rozwiązań: **Dionaea**, **Glastopf**, **Kippo** oraz **Honeyd** zostały zidentyfikowane jako najbardziej użyteczne i najłatwiejsze do zainstalowania. Dla podmiotów mogących przeznaczyć większą ilość środków na utrzymanie honeypotów – w zamian zyskując zdolność wykrywania złośliwych stron WWW – warto zapoznać się z klienckim honeypotem Thug oraz Capture-HPC NG.

Poza określeniem użyteczności poszczególnych honeypotów typu standalone, sprawdziliśmy też rozwiązania online oraz sandboksy. Zbadaliśmy również rozwiązania, które korzystają z honeypotów, np. do wczesnego ostrzegania, narzędziach wspomagających, a także określiliśmy różne strategie ich wdrożenia. Wskazaliśmy na słabe punkty technologii honeypot i zaproponowaliśmy szereg rekomendacji, które mogą pomóc w ich szerszej aplikacji. Dodatkowo, wskazaliśmy możliwe kierunki rozwoju. Raportowi towarzyszy opracowane przez nas ćwiczenie, umożliwiając nauczenie się obsługiwania i przeprowadzania analiz za pomocą technologii honeypotowych.

Podsumowując, honeypoty stanowią ważne narzędzie w arsenale zespołów typu CERT. Oferują wgląd w ataki w sieci, zapewniając usługę wczesnego ostrzegania o infekcji i zachowaniu złośliwego oprogramowania, są również doskonałą platformą do dowiedzenia się o zmianach w taktyce atakujących. Mogą być wykorzystane jako podstawa do tworzenia dużych systemów opartych o sieci sensorów lub jako dodatkowe źródło dla już wdrożonych narzędzi SIEM.

Zachęcamy do zapoznania się z pełnym raportem pod adresem http://bit.ly/UqvBqp (**http://www.enisa.europa.eu/activities/cert/support/proactive-detection-of-security-incidents-II-honeypots**), mając nadzieję, że przyczyni się on do popularyzacji i rozwoju technologii typu honeypot.

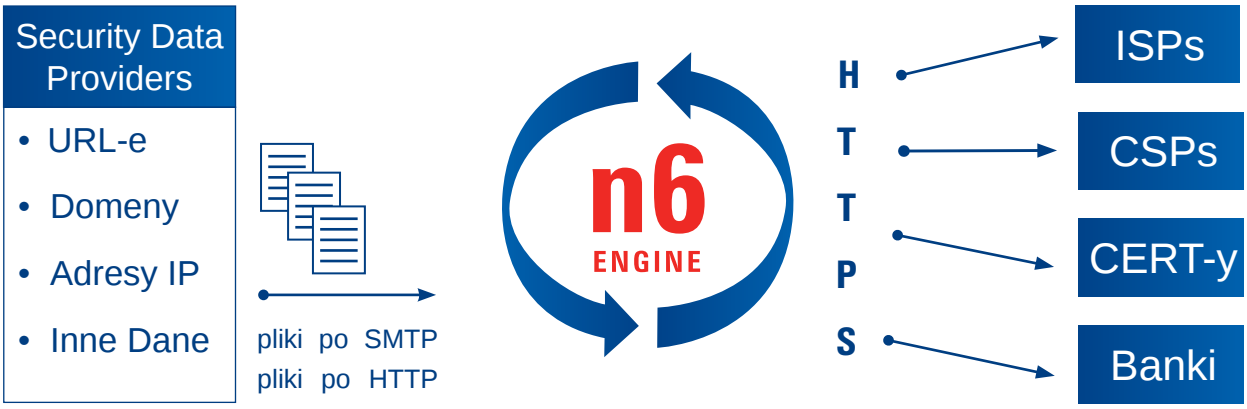
5.5 n6 - platforma wczesnego ostrzegania o incydentach w sieci

W lutym 2012 roku została uruchomiona, zbudowana w całości przez CERT Polska, platforma służąca do gromadzenia, przetwarzania i przekazywania informacji o zdarzeniach bezpieczeństwa w sieci. Platforma n6 (network security incident exchange) to jeden z kluczowych projektów bezpieczeństwa realizowanych przez CERT Polska. W ciągu jednego roku w ramach n6 przetwarzane są dziesiątki milionów zdarzeń z Polski i całego świata.

Głównym celem n6 jest efektywne, niezawodne i szybkie dostarczenie dużych ilości informacji o zagrożeniach bezpieczeństwa właścicielom, administratorom i operatorom sieci. Dane trafiają do n6 poprzez wiele kanałów dystrybucyjnych dostarczających informacji o zdarzeniach bezpieczeństwa.

Zdarzenia te wykrywane są w wyniku działań systemów wykorzystywanych przez różne podmioty zewnętrzne (takie jak inne zespoły CERT, organizacje bezpieczeństwa, producenci oprogramowania, niezależni eksperci itp.) oraz systemów monitorowania obsługiwanych przez CERT Polska. Dane są zawsze dystrybuowane za zgodą podmiotów, które wykryły zdarzenie, natomiast samo źródło jest ujawniane tylko w przypadku, kiedy samo wyrazi na to zgodę.

Działanie platformy n6 można porównać do sortowni incydentów. Dzięki rozbudowanemu systemowi tagowania, incydenty mogą być przypisywane do podmiotów, których dotyczą na podstawie adresów IP i numerów AS. Dane są agregowane w przygotowaną indywidualnie dla odbiorcy paczkę, która zachowuje oryginalny format źródła. Istnieje również możliwość dostarczania informacji nieznajdujących się w danej sieci, ale które mogą zostać przez jej właściciela wykorzystane do wykrywania u siebie zainfekowanych komputerów (jak np. dane o serwerach C&C). Większość informacji aktualizowanych jest codziennie, niektóre częściej.



Rysunek 29. Schemat działania platformy n6

Przykładowe zbiory danych znajdujące się w platformie n6:

- złośliwe adresy URL
- złośliwe oprogramowanie i inne artefakty
- zainfekowane hosty (boty)
- serwery C&C
- skanowania
- DDoS
- ataki bruteforce
- uczestnictwo w sieci fast flux
- phishing
- spam
- dane specjalne (w wyniku działań operacyjnych CERT Polska)

Specjalnym źródłem informacji o danej sieci mogą być wyniki działań operacyjnych CERT Polska. Przykładami takich danych, które udostępniliśmy w 2012 roku, są dane dotyczące komputerów zainfekowanych Zeusem P2P, dane z działalności botnetu Ramnit oraz dane komputerów, które połączyły się z sinkholem przeznaczonym dla botów Kelihos.B. Dane specjalne mogą również pochodzić z działań operacyjnych innych podmiotów – takie otrzymane jednorazowo dane z zewnątrz, za zgodą źródła mogą być dodawane do systemu w celu redystrybucji.

W platformie przekazywane są informacje o źródłach ataku w postaci adresów URL, domen, adresów IP lub nazw złośliwego oprogramowania, a także, w zależności od dostępności, informacje o danych specjalnych. Ponieważ większość danych pochodzi z systemów zewnętrznych, należy pamiętać, że są one przekazywane w postaci nieprzetworzonej i mogą zawierać fałszywe alarmy. Weryfikacja danych zależy wyłącznie od odbiorcy.

W n6 uczestniczy już ponad 100 właścicieli sieci, operatorów i administratorów, którzy na co dzień otrzymują dane o zagrożeniach w swojej infrastrukturze. Zapraszamy wszystkie osoby które chciałyby otrzymywać informacje z n6 do zgłoszenia się do CERT Polska. Dostęp do n6 jest bezpłatny i nie wymaga instalacji jakichkolwiek sond w sieci ani oprogramowania. Więcej informacji na temat n6 wraz z instrukcją jak przystąpić do projektu, znajduje się na stronie http://n6.cert.pl.

6. Raport ARAKIS

6.1 Wstęp

System ARAKIS jest projektem zespołu CERT Polska działającego w strukturach instytutu badawczego NASK. System rozwijany jest we współpracy z Działem Rozwoju Oprogramowania oraz z Działem Naukowym instytutu. Głównym zadaniem systemu jest wykrywanie i opisywanie zagrożeń występujących w sieci na podstawie agregacji i korelacji danych z różnych źródeł, w tym rozproszonej sieci honeypotów, darknet, firewalli oraz systemów antywirusowych. W przypadku podstawowego źródła danych – honeypotów – system bazuje na danych pozyskanych z ruchu **nieprodukcyjnego**. W związku z tym nie jest możliwe wykrywanie i analizowanie ataków precyzyjnych wycelowanych jedynie w serwery produkcyjne (np. DDoS). ARAKIS sprawdza się natomiast w analizowaniu zagrożeń (głównie automatycznych) propagujących się poprzez aktywne skanowanie sieci (w takim przypadku jest duża szansa, że zostanie nawiązane połączenie do honeypota), np. robaki sieciowe.

Szczególną implementacją systemu ARAKIS jest projekt ARAKIS-GOV wykorzystywany do ochrony zasobów teleinformatycznych administracji publicznej. Jest on obecnie wdrożony w ponad siedemdziesięciu instytucjach administracji publicznej we współpracy z polskim zespołem rządowym CERT.GOV.PL działającym w strukturach Departamentu Bezpieczeństwa Teleinformatycznego ABW.

Niniejsze roczne podsumowanie jest piątym tego typu w historii systemu. W raporcie zamieszczono m.in. statystyki dotyczące źródeł zagrożeń, najczęściej skanowanych portów i usług, oraz rodzajów zagrożeń według reguł systemu IDS Snort. Ponadto opisano interesujący przypadek anomalii w sieci BitTorrent, która została zaobserwowana przez system ARAKIS. W tym roku zrezygnowaliśmy ze statystyk alarmów generowanych przez system, ponieważ ich liczba nie odzwierciedla bezpośrednio poziomu zagrożenia – alarmy jedynie zawiadamiają operatorów o pewnym zdarzeniu w systemie.

6.2 Statystyki dotyczące ataków

Jedną z ważniejszych kategorii związanych z atakami wykrywanymi przez honeypoty systemu ARAKIS jest skanowanie portów. Ranking przedstawia liczbę unikalnych w skali całego roku adresów IP, które próbowały łączyć się na poszczególne porty. Obrazuje to bezpośrednio skalę zainteresowania konkretnymi portami (a więc usługami słuchającymi na nich) przez złośliwe oprogramowanie bądź narzędzia typu skanery bezpieczeństwa.

Na pierwszym miejscu znajduje się port 23/TCP związany z usługą Telnet. Na drugim miejscu jest 445/TCP – na nim nasłuchuje wiele aplikacji związanych z oprogramowaniem Microsoft, które miało wiele efektownych luk wykorzystywanych przez takie robaki, jak Sasser czy Conficker. W stosunku do zeszłego roku porty te zamieniły się miejscami, a port 445/TCP nie znajduje się na szczycie listy po raz pierwszy

odkąd publikujemy statystyki z systemu ARAKIS. Na trzecim miejscu znajduje się port 3389/TCP związany z połączeniami RDP (używany jest przez windowsową usługę „zdalny pulpit" oraz wykorzystującego ją robaka Morto).

Pozycja	Liczba unikalnych IP per rok	Docelowy port/ protokół	Zmiana w stosunku do roku 2011	Opis ataków występujących na porcie
1	69869	23/TCP	▲ 1	Ataki na usługę telnet
2	54383	445/TCP	▼ 1	Ataki typu buffer overflow na usługi Windows RPC
3	26661	3389/TCP	▲ 5	Ataki słownikowe na RDP (zdalny pulpit) – w dużej mierze aktywność robaka Morto
4	25238	22/TCP	0	Ataki słownikowe na usługę SSH
5	15050	139/TCP	0	Ataki na usługę NetBIOS / współdzielenie plików i drukarek
6	14795	80/TCP	▲ 1	Ataki na aplikacje webowe
7	10729	1433/TCP	▼ 1	Ataki na MS SQL
8	9779	135/TCP	▼ 5	Ataki na windowsową usługę DCE/RPC
9	6544	25/TCP	▲ 2	Skanowania w poszukiwaniu serwerów pocztowych typu open relay
10	6280	8080/TCP	▲ 1	Skanowania w poszukiwaniu serwerów open web proxy lub ataki na aplikacje webowe

Tabela 22. Najczęściej atakowane porty

Innym ciekawym zestawieniem są statystyki Top 10 najczęściej dopasowanych reguł systemu Snort. W tym przypadku także wyznacznikiem były unikalne w skali roku źródłowe adresy IP. W stosunku do roku poprzedniego pierwsze cztery miejsca klasyfikacji nie uległy zmianie – jedynie zwiększyła się liczba widzianych unikalnych adresów IP, z których przeprowadzano ataki. Podobnie jak w roku ubiegłym wszystkie reguły poza jedną (związaną ze słownikowymi atakami na usługę SSH) dotyczą ataków na usługi windowsowe. Jednocześnie ta jedna reguła opisująca ataki na SSH „awansowała" w rankingu o największą liczbę pozycji równą cztery.

Pozycja	Reguła Snort	Zmiana w stosunku do roku 2011	Liczba unikalnych IP
1	ET POLICY RDP connection request	0	174504
2	MISC MS Terminal server request	0	164714
3	ET POLICY Radmin Remote Control Session Setup Initiate	0	95174
4	ET SCAN DCERPC rpcmgmt ifids Unauthenticated BIND	0	32116
5	ET SCAN Potential SSH Scan	▲ 4	26838
6	ET POLICY Suspicious inbound to MSSQL port 1433	▲ 1	24122
7	NETBIOS SMB-DS IPC$ unicode share access	▲ 1	21144
8	ATTACK-RESPONSES Microsoft cmd.exe banner	▼ 3	20905
9	ET EXPLOIT MS04011 Lsasrv.dll RPC exploit (WinXP)	▲ 2	20031
10	ET EXPLOIT LSA exploit	0	20031

Tabela 23. Najczęściej dopasowywane reguły Snort

W statystykach opisujących geograficzne położenie źródeł ataków na pierwszym miejscu znajdują się Chiny. Dotyczy to zarówno zestawienia liczby unikalnych adresów IP, jak i liczby wszystkich połączeń. W 2011 roku atakujących unikalnych adresów IP najwięcej było z USA, natomiast Chiny plasowały się na czwartej pozycji. W roku 2012 Chiny wyprzedziły pozostałe kraje zwiększając prawie trzykrotnie liczbę obserwowanych ataków z unikalnych adresów IP. Jednocześnie liczba wszystkich podejrzanych połączeń z Chin również zwiększyła się – w tym wypadku ponad dwukrotnie. Oprócz Chin szczególnie rosnącą liczbę zagrożeń odnotowaliśmy także z krajów: USA, Zjednoczone Emiraty Arabskie, Niemcy oraz Indie. Natomiast zmniejszyła się liczba zagrożeń pochodzących z Polski, Ukrainy i Korei Południowej.

Pozycja	Kraj	Zmiana w stosunku do roku 2011	Liczba unikalnych adresów IP
1	CN	▲ 4	33762
2	US	▼ 1	30840
3	TR	0	15101
4	RU	▼ 2	15094
5	AE	▲ 4	15094
6	TW	▲ 1	10423
7	DE	▲ 3	9007
8	IN	▲ 17	7521
9	UA	▼ 1	6883
10	KR	▼ 6	6133

Tabela 24. Najbardziej zainfekowane kraje pod względem unikalnych adresów IP

Pozycja	Kraj	Zmiana w stosunku do roku 2011	Liczba połączeń
1	CN	0	4865733
2	US	0	3826534
3	RU	0	811973
4	DE	▲ 4	688854
5	KR	0	486521
6	TR	0	478638
7	UA	▼ 3	442061
8	TW	▲ 1	421963
9	GB	▲ 1	402343
10	FR	▲ 1	401807

Tabela 25. Najbardziej zainfekowane kraje pod względem liczby przepływów

Zestawienie najbardziej zainfekowanych systemów autonomicznych ujawnia, że najwięcej unikalnych adresów IP atakowało z sieci chińskiego operatora Chinanet (AS4134). Ponadto duży skok w niechlubnym rankingu zanotował inny chiński operator (AS4837) oraz indyjski Tata Communications (AS17908), który „awansował" w stosunku do klasyfikacji z roku 2011 aż o 412 miejsc.

Pozycja	Zmiana w stosunku do roku 2011	Liczba unikalnych adresów IP	Numer AS	Kraj	Nazwa operatora
1	▲ 5	17603	AS4134	CN	CHINANET-BACKBONE No.31,Jin-rong Street
2	▼ 1	11922	AS9121	TR	TTNET Turk Telekomunikasyon Anonim Sirketi
3	0	10682	AS5384	AE	EMIRATES-INTERNET Emirates Telecommunications Corporation
4	▲ 1	8121	AS3462	TW	HINET Data Communication Business Group
5	▲ 9	5552	AS4837	CN	CNCGROUP China169 Backbone
6	▲ 1	3080	AS6147	PE	Telefonica del Peru S.A.A.
7	▼ 3	3051	AS12741	PL	Netia SA
8	▼ 6	2738	AS4766	KR	KIXS-AS-KR Korea Telecom
9	0	2663	AS24863	EG	LINKdotNET-AS
10	▲ 412	2503	AS17908	IN	TCISL Tata Communications

Tabela 26. Najbardziej zainfekowane systemy autonomiczne pod względem unikalnych adresów IP

W zestawieniu liczby połączeń bez uwzględnienia unikalności nadawcy aż trzy pierwsze pozycje zajmują operatorzy chińscy! Na czwartym miejscu pojawił się amerykański operator, który przeskoczył w rankingu aż o 36 miejsc. Ogólnie w pierwszej dziesiątce największej liczby podejrzanych połączeń znajduje się aż pięć operatorów chińskich i dwóch amerykańskich.

Pozycja	Zmiana w stosunku do roku 2011	Liczba połączeń	Numer AS	Kraj	Nazwa operatora
1	0	2040530	AS4134	CN	CHINANET-BACKBONE No.31,Jin-rong Street
2	0	875613	AS4837	CN	CHINA169-BACKBONE CNCGROUP China169 Backbone
3	▲ 2	401613	AS23650	CN	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province backbone
4	▲ 36	397591	AS32475	US	SINGLEHOP-INC - SingleHop
5	▲ 3	327697	AS3462	TW	HINET Data Communication Business Group
6	▼ 3	292274	AS9121	TR	TTNET Turk Telekomunikasyon Anonim Sirketi
7	▲ 4	238063	AS4812	CN	CHINANET-SH-AP China Telecom (Group)
8	▲ 26	218162	AS4808	CN	CHINA169-BJ CNCGROUP IP network China169 Beijing Province Network
9	0	202472	AS36351	US	SOFTLAYER - SoftLayer Technologies Inc.
10	▼ 4	184133	AS5384	AE	EMIRATES-INTERNET Emirates Telecommunications Corporation

Tabela 27. Najbardziej zainfekowane systemy autonomiczne pod względem liczby przepływów

Poniżej znajduje się rozkład zainfekowanych IP w polskich sieciach. Ogólnie liczba widzianych unikalnych adresów IP pochodzących z polskich sieci spadła. Największy, ponad dwukrotny spadek obserwowanych zagrożeń zauważono w sieci Netia (AS12741). Niestety operator ten nadal znajduje się na pierwszym miejscu w tej niechlubnej klasyfikacji ze sporą przewagą – i to pomimo faktu, że liczba unikalnych IP z trzech następnych w klasyfikacji sieci (UPC, TP oraz OVH) znacząco wzrosła.

Pozycja	Zmiana w stosunku do roku 2011	Liczba unikalnych adresów IP	Numer AS	Nazwa operatora
1	0	3051	AS12741	Netia
2	▲ 19	1887	AS6830	UPC
3	▼ 1	1148	AS5617	TP
4	nowy	1142	AS16276	OVH
5	▼ 2	226	AS21021	Multimedia
6	0	68	AS29314	Vectra
7	nowy	52	AS56475	DATA-COM
8	▲ 5	51	AS25388	ASK-NET
9	nowy	50	AS43929	ASN
10	0	44	AS6714	GTS

Tabela 28. Zainfekowane adresy IP w polskich sieciach

6.3 Interesujące przypadki zaobserwowanych incydentów sieciowych

Oprócz ochrony, jaką system ARAKIS zapewnił sieciom, w których zainstalowane są sondy, przyczynił się także do ciekawych obserwacji zjawisk i trendów związanych z ruchem w Internecie. W skrócie opisana została najciekawsza, naszym zdaniem, obserwacja nie związana bezpośrednio z ochroną sieci uczestników projektu. Dotyczyła ona anomalii w sieci BitTorrent.

Anomalia w ruchu uTP

W kwietniu 2012 roku obserwowaliśmy znaczny wzrost aktywności w sieci BitTorrent (opartej na protokole uTP). Niektóre z rejestrowanych pakietów wywoływały fałszywe alarmy systemu ARAKIS wysokiego poziomu informujące o możliwej infekcji chronionych węzłów. Co więcej, z danych dotyczących ruchu wynikało między innymi, że występowała komunikacja pomiędzy dwiema sondami systemu ARAKIS, co było bardzo mało prawdopodobne (sondy są pasywne i same z siebie nie nawiązują połączeń). Oznaczało to, że adresy zawarte w pakietach IP składających się na ten ruch były błędne (najprawdopodobniej podrobione).

6.3.1 Co to jest uTP?

Protokół uTP wykorzystuje do transportu protokół UDP i uzupełnia go o funkcje protokołów połączeniowych. Obudowuje on (lub inaczej: enkapsuluje) zwykłe pakiety BitTorrent (BT). Oznacza to, że zwykły ruch BitTorrentowy znajduje się wewnątrz kanału komunikacyjnego utworzonego w warstwie uTP. Kanał ten posiada niektóre z właściwości kanału TCP, takie jak na przykład zorientowanie na połączenie i jego kontrolę. Zwykłe pakiety BitTorrentowe korzystają z cech protokołu TCP, takich jak potwierdzanie odbioru danych, regulowanie wielkości okna etc., natomiast w tym przypadku własności te zapewnia uTP. Po co więc kolejny protokół, skoro można korzystać z TCP? Otóż stos UDP/uTP/BT ma za zadanie m.in. zwiększenie kontroli nad obciążeniem. Prędkość ściągania danych z Internetu przez klienta BitTorrent nie podlega takim ograniczeniom, jak transmisja z serwerów FTP i HTTP (czyli ograniczeniu pasma po stronie serwera). Dlatego przy pobieraniu dużych ilości danych może zdarzyć się, że w sieci klienta wystąpi obciążenie wysycające większość lub całe dostępne pasmo, uniemożliwiając jej poprawne funkcjonowanie. Jednym z rozwiązań jest zastosowanie ograniczeń transferu na poziomie aplikacji klienta. Nie są to bardzo rozbudowane funkcje, wielu użytkowników o nich nie pamięta. uTP natomiast pozwala na dynamiczne regulowanie przepustowości w sieci BT na poziomie protokołu i dodatkowo posiada inne możliwości, jak wspomaganie transferu u klientów o wąskim paśmie czy dzielenie linii ADSL z przeglądarką internetową.

6.3.2 Nasze obserwacje uTP (statystyki)

Z posiadanych przez nas danych wynika, że aktywność sieci uTP, a co za tym idzie – również BT – znacznie wzrosła w pierwszych miesiącach roku 2012 w porównaniu do roku 2011. Wybraliśmy do analizy próbkę ruchu z 1. kwietnia roku 2011 i tego samego dnia roku 2012, w tej samej lokalizacji.

	01-04-2011	01-04-2012
Liczba wszystkich pakietów:	103546 (8.7MB)	2142296 (201MB)
Liczba pakietów UDP:	183 (~0.2% ruchu)	957047 (~45% ruchu)
Anomalia:	393862 (~18% całego ruchu i ~41% ruchu UDP)	

Tabela 29. Zestawienie statystycznych parametrów analizowanego ruchu.

Przy tworzeniu tego zestawienia przyjęto założenie, że analizowany ruch (pakiety składające się na anomalię) to ruch złożony z pakietów o charakterystyce podobnej do tych, które wywołały fałszywe alarmy w systemie ARAKIS.

Wyznaczona charakterystyka jest następująca:

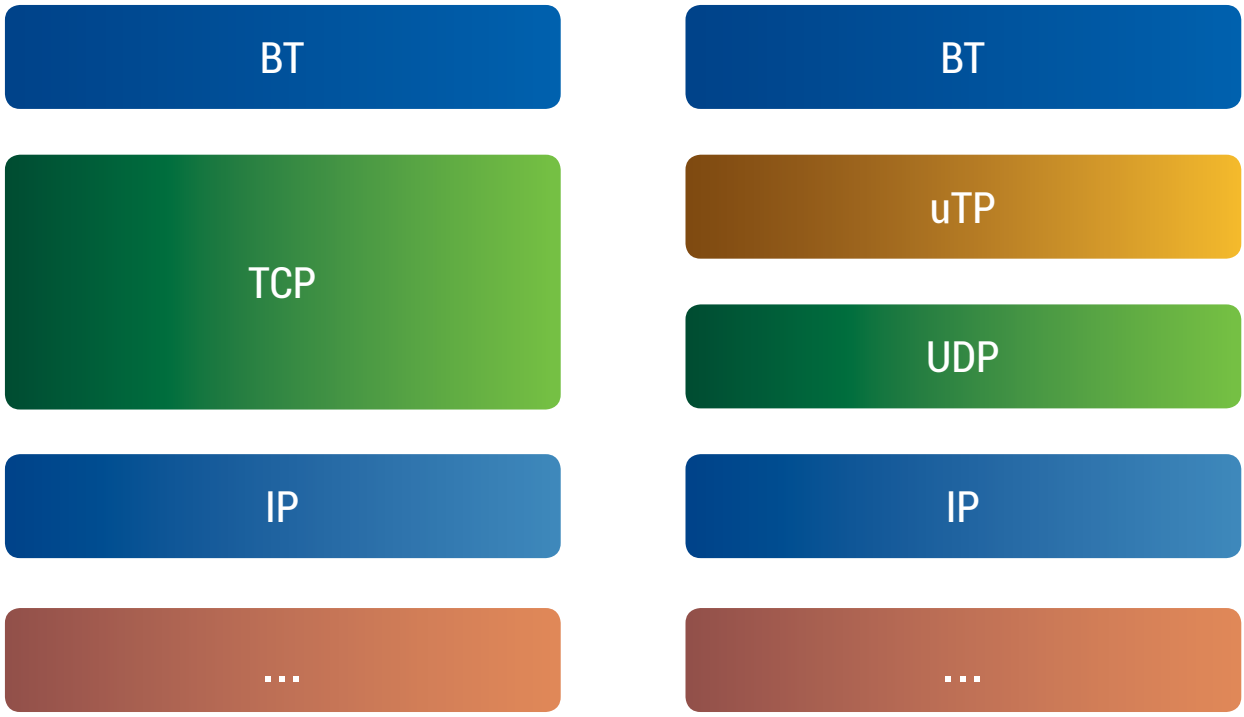
- Pakiet wywołujący anomalię jest pakietem uTP z ustawioną flagą DATA.
- Pakiet ten zawiera pakiet BT, który zawiera następujące informacje:
  - Hash protokołu BitTorrent: `057a315b89b54e53e2ee583dd5cd9ef60648805e`
  - Peer protokołu BitTorrent: `0000000000000000000000000000000000000000`

Można trochę osłabić te założenia i przyjąć, że na ruch-anomalię składają się także pakiety uTP SYN, które poprzedzają pakiety DATA, o takim samym porcie źródłowym i docelowym jak pakiety DATA. Wtedy podsumowanie z 1. kwietnia 2012 roku wygląda następująco: **anomalia = 787724 (~37% całego ruchu i ~82% ruchu UDP)**. Jeżeli dodać do tego pakiety ICMP informujące o zamkniętym porcie UDP, które zwracała sonda, statystyka staje się już bardzo znacząca: **anomalia = 1575448 (~73% całego ruchu)**.

Można łatwo zauważyć, że udział ruchu uTP jest nieproporcjonalnie duży w stosunku do reszty protokołów, jeśli porównać go do próbki z 2011 roku. Jest to także ponad 20-krotny przyrost całości ruchu. Podobne symptomy anomalii obserwowaliśmy w różnych lokalizacjach rozproszonej sieci sond.

6.3.3 Analiza pakietów

Poniżej przedstawiamy poglądową ilustrację porównawczą klasycznego stosu BitTorrent i stosu uTP. Stopniowo przeanalizujemy informacje zawarte w poszczególnych warstwach.



Rysunek 30. Porównanie stosów protokołów BT i uTP

Warstwa IP/UDP

Zacznijmy od warstwy IP/UDP. Poniżej znajduje się zestawienie źródłowych i docelowych adresów i portów analizowanych transmisji (ruch przychodzący uTP).

Liczba	Adres IP
613	xxx.xxx.192.40
463	xxx.xxx.67.237
463	xxx.xxx.17.54
459	xxx.xxx.115.38
373	xxx.xxx.40.233
367	xxx.xxx.158.104
362	xxx.xxx.183.36
360	xxx.xxx.177.102
360	xxx.xxx.102.55
347	xxx.xxx.221.41

Tabela 30. Top 10 - adresy źródłwe.

Liczba	Adres IP
393850	xxx.xxx.xxx.34
4	xxx.xxx.xxx.27

Tabela 31. Adresy docelowe (wszystkie z próbki).

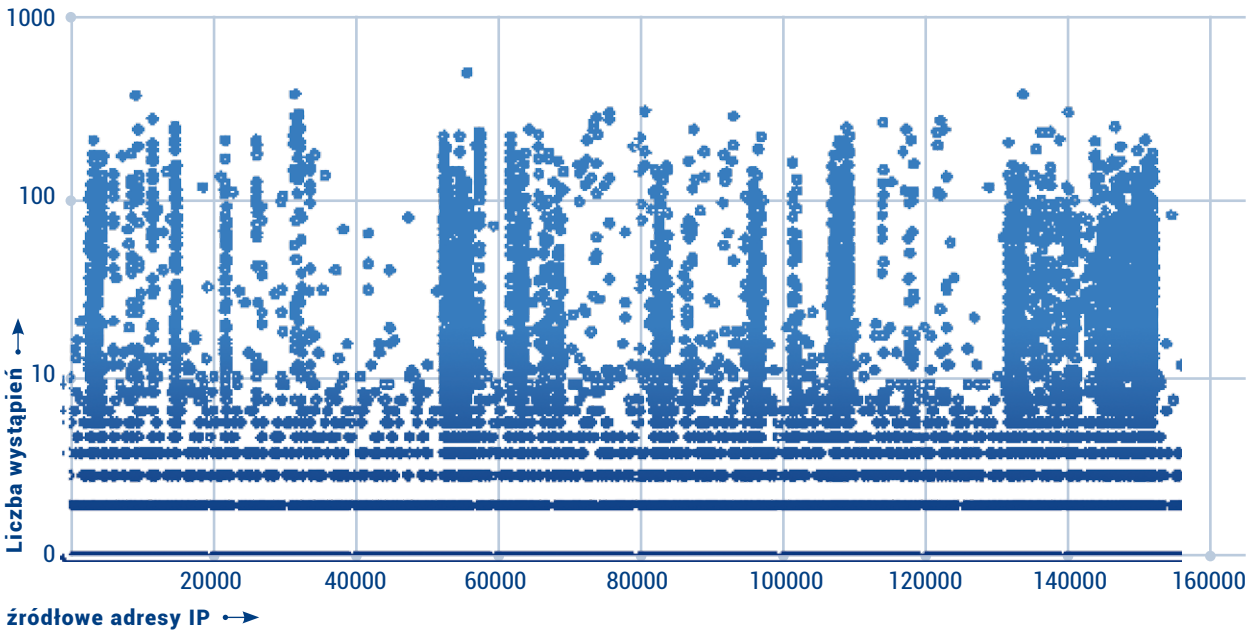
Liczba	Port
133014	45571
79677	62100
39658	60598
35461	55025
30830	47013
29605	45770
11555	36610
9697	57902
5996	20995
4989	32692

Tabela 32. Top 10 - porty źródłwe.

Liczba	Port
133007	45571
79672	62100
39657	60598
35461	55025
30829	47013
29604	45770
11554	36610
9697	57902
5996	20995
4989	32692

Tabela 33. Top 10 - porty docelowe.

Jeśli pominąć wyróżniające się adresy znajdujące się na szczycie listy, adresy źródłowe posiadają dość równomierny rozkład. Pochodzą z różnych systemów AS i różnych lokalizacji geograficznych (w tym: z Rosji, Kanady, Chin, Australii, USA). Rozkład tych adresów posiada cechy sumy rozkładu równomiernego i pewnego rozkładu nierównomiernego. Może to oznaczać, że część tych adresów jest wykorzystywana w równomierny sposób (np. po kolei) lub są losowane (tj. podrabiane).



Rysunek 31. Rozkład źródłowych adresów IP

Zróżnicowany rozkład geograficzny adresów źródłowych skłania do przyjęcia raczej drugiego wytłumaczenia. Niewykluczone, że wykorzystywana jest również jakiegoś rodzaju rozproszona sieć anonimizująca. Wyrywkowo wybrane węzły nie przeszły testów na węzły sieci TOR, jednak pozostają jeszcze inne możliwości: inne rozproszone sieci anonimizujące, usługi VPN, botnety.

W przypadku źródłowych i docelowych portów transmisji można zauważyć, że preferowane są wysokie porty. Podobne porty są wybierane jako źródło i cel transmisji.

Warstwa uTP

Ruch przychodzący, składający się na anomalię, można przedstawić jako serie przepływów z różnych źródeł złożonych z dwóch pakietów uTP: uTP SYN i uTP DATA. Pakiety te składają się na opisywany w protokole uTP mechanizm nawiązywania połączenia (handshake), jednak pewne ich cechy są niezgodne z protokołem. Oto one:

- **Źródło transmisji ignoruje pakiety ICMP informujące o zamkniętym porcie.**
  W specyfikacji protokołu uTP nie jest opisana poprawna reakcja na wiadomości ICMP. Jednak klient uTP próbujący nawiązać połączenie powinien poprawnie zinterpretować tą wiadomość i uznać nawiązanie połączenia jako niemożliwe.
- **Źródło transmisji ignoruje brak pakietu uTP STATE i wysyła pakiet DATA.**
  Bez pakietu STATE nie posiada ono poprawnego numeru potwierdzenia, zatem nawiązanie połączenia jest niemożliwe. Zamiast poprawnego numeru potwierdzenia umieszcza on w tym miejscu 0, co stanowi odstępstwo od protokołu. W trakcie badań wysyłaliśmy pakiety o podobnej konstrukcji do klienta uTorrent, odpowiadał on pakietem FIN i kończył konwersację. Przypuszczamy, że jest to efekt nieprzestrzegania protokołu.

Inne interesujące lub niezwykłe cechy pakietów uTP:

- Większość pakietów w polu timestamp difference ma wartość 0.
- Większość pakietów w polu window size ma wartość 0x380000 (3670016 w systemie dziesiętnym).

Liczba	Wartość hex
392850	00 00 00 00
10	6f 63 6f 6c
4	fd 7a 9f f1
4	Fb 26 16 d3
4	fa 5b c0 83
4	f9 e9 d8 6d
4	f9 46 4a 14
4	f9 37 8d f9
4	f8 3c a3 1a
4	f6 9a ec df

Tabela 34. Wartości timestamp difference microseconds (Top 10):

Liczba	Wartość hex
393017	00 38 00 00
738	00 04 00 00
50	00 00 00 00
46	00 03 20 00
4	00 03 99 99
4	00 03 33 33
4	00 00 13 02
3	00 01 93 7c
3	00 00 0e 32
2	00 02 1d fd

Tabela 35. Wartość window size - Top 10.

Wartości pól *timestamp microseconds* w dwóch pakietach w tych samych przepływach różni się o wielokrotność 10000 mikrosekund.

Część tych właściwości może wynikać z konkretnych implementacji protokołu, ale inne sprawiają, że stosowanie tego protokołu traci sens. Jest bardzo mało prawdopodobne, że przy tak wysokiej rozdzielczości tak schematyczne wartości w polu *timestamp microseconds* były zgodne z rzeczywistością. Jeśli te wartości są sfałszowane, protokół traci swoje możliwości kontroli konsumpcji pasma i jego stosowanie w tym celu nie ma sensu.

Warstwa BitTorrent

W pakietach BT znajduje się hash: `057a315b89b54e53e2ee583dd5cd9ef60648805e`. Dotyczy on informacji o plikach wideo zawierających film „Avgust. Vosmogo". Jest to rosyjski film akcji, który swoją premierę miał 21. lutego 2012 roku. Przy analizowaniu ruchu z sond z innych lokalizacji zarejestrowaliśmy podobne pakiety zawierające hashe dotyczące informacji o innych plikach posiadajacych wspomniany film oraz plikach z innym rosyjskim filmem: „Shpion" (więcej o znaczeniu pola hash: http://wiki.theory.org/BitTorrentSpecification#Tracker_Request_Parameters).

Poniżej przedstawiamy interesujące korelacje czasowe pomiędzy publikacją torrentów, a transmisjami zawierającymi odpowiadające im hashe:

Hash	Data publikacji torrenta	Data zarejestrowanych transmisji
`c11ba392ef3dd57942112641ce8f1d9b96f0ddd5`	26.02.2012	17.03.2012
`057a315b89b54e53e2ee583dd5cd9ef60648805e`	17.03.2012	01.04.2012

W badanym ruchu z 1. kwietnia 2012 roku 99.99% pakietow uTP DATA zawierało hash `057a315b89b54e53e2ee583dd5cd9ef60648805e`.

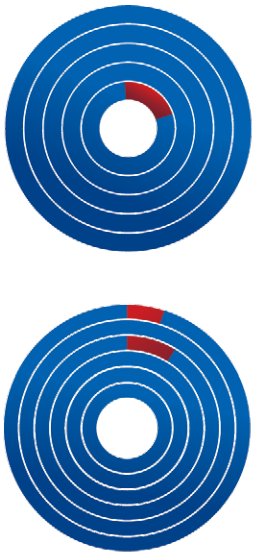
Omawiane pakiety zawierały również identyfikatory peerów BT (więcej o znaczeniu tego pola: http://wiki.theory.org/BitTorrentSpecification#peer_id).

Liczba	Peer ID
329755	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
399	2d54 5232 3432 302d xxxx xxxx xxxx xxxx xxxx xxxx
214	2d54 5232 3530 302d xxxx xxxx xxxx xxxx xxxx xxxx
213	2d54 5232 3432 302d xxxx xxxx xxxx xxxx xxxx xxxx
100	2d55 5432 3231 302d xxxx xxxx xxxx xxxx xxxx xxxx
97	2d55 5431 3737 302d xxxx xxxx xxxx xxxx xxxx xxxx
95	2d54 5231 3933 302d xxxx xxxx xxxx xxxx xxxx xxxx
93	2d54 5231 3933 302d xxxx xxxx xxxx xxxx xxxx xxxx
91	2d55 5433 3132 302d xxxx xxxx xxxx xxxx xxxx xxxx
90	2d4d 4732 3125 302d xxxx xxxx xxxx xxxx xxxx xxxx

Tabela 36. Wartość pola peer ID - Top 10

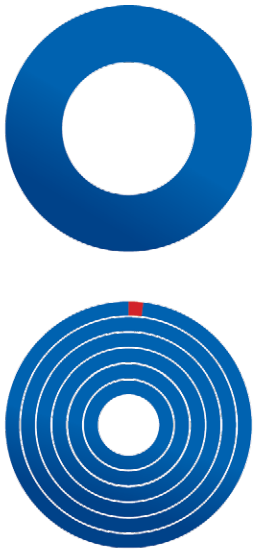
Jak widać, większość pakietów zawierała w tym polu ciąg zer.

Avgust. Vosmogo



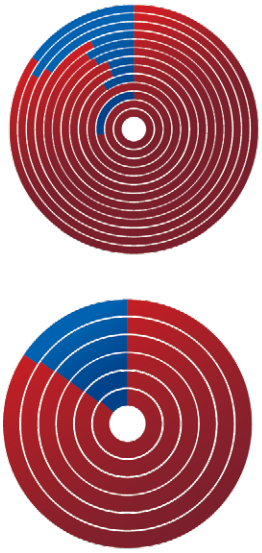
Rysunek 33. Statystyki seederów/leecherów per tracker dla torrenta o hashu
c11ba392ef3dd57942112641ce8f1d9b96f0ddd5

Avgust. Vosmogo



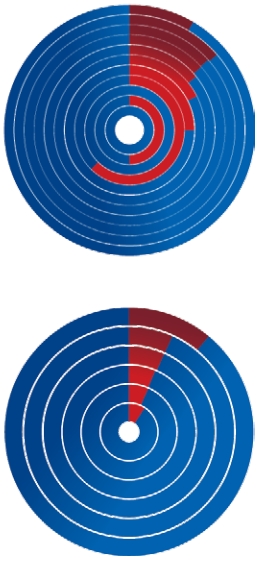
Rysunek34. Statystyki seederów/leecherów per tracker dla torrenta o hashu
ab53cb0d665b34fcdf1939b271660b48297b5a74

Lost



Rysunek35. Statystyki seederów/leecherów per tracker dla torrenta o hashu
799db5ad3c746823a8df170bb1a717835c1dccc8

Naruto



Rysunek 36. Statystyki seederów/leecherów per tracker dla torrenta o hashu
057a315b89b54e53e2ee583dd5cd9ef60648805e

seeders leechers

Powyżej prezentujemy statystyki rozkładu leecherów i seederów dotyczących omawianych torrentów uzyskane od popularnych trackerów torrentowych (m.in. torrentproject.com, torrentz.eu i bitsnoop.com).

Na rysunku można zauważyć małą liczbę leecherów. Dla porównania przedstawiamy statystyki dotyczące innych torrentów, bardzo popularnych (dot. serialu Lost) i mniej popularnych (Naruto) – zostały te same trackery.

Statystyki dotyczące badanych torrentów posiadają w większości wielu seederów i bardzo mało (najczęściej – 0) leecherów. Jest to raczej niezwykły rozkład. W większości „normalnych" przypadków proporcje – jeśli nie są zupełnie odwrotne – to nie są aż tak wyraźne.

6.3.4 Hipotezy

Nie udało się jednoznacznie ustalić przyczyn i skutków ruchu składającego się na anomalie występujące w naszych sieciach honeynetów. Oto kilka zebranych hipotez dot. tego ruchu.

Źródła anomalii

Zidentyfikowaliśmy pięć potencjalnych źródeł anomalii:

- **Adresy źródłowe są podrobione.**

Taką możliwość potwierdza równomierny charakter jednego ze składników rozkładu adresów oraz – przede wszystkim – adresy źródłowe, należące do naszych honeynetów, w których żadne węzły nie inicjują transmisji.

- **Adresy źródłowe są prawdziwe**.

W trakcie dokładniejszego badania odnaleźliśmy połączeniową sesję TCP z pakietami BT częściowo odpowiadającym charakterystyce (posiadają taki sam hash). Nawiązanie sesji TCP za pomocą podrobionych adresów źródłowych IP jest bardzo trudne i praktycznie niemożliwe w sieciach WAN, dlatego można przypuszczać, że adres źródłowy tej transmisji był prawdziwy. Jest również bardzo mało prawdopodobne (głównie ze względu na korelację czasową), że wspomniana sesja była niezwiązana z anomalią. Zawierała podobny pakiet BT (ten sam hash), jednak zawierała też niezerową wartość peera. Niewykluczone, że pod adresem tym funkcjonował zwykły klient uTP lub BT.

- **Pula adresów źródłowych zawiera zarówno adresy prawdziwe, jak i podrobione.**

Najbardziej prawdopodobna możliwość.

- **Porty źródłowe i docelowe to standardowe porty dla konwersacji uTP.**

Z obserwacji poczynionych w trakcie badań z klientem uTorrent wynika, że ten klient domyślnie oczekuje na połączenia na porcie 12144. Może on zostać zmieniony przez użytkownika lub wylosowany. Porty transmisji mogły zostać wyznaczone na podstawie obserwacji publicznych trackerów.

- **Źródłem transmisji nie jest zwykły klient uTP, tylko inny program lub skrypt służący innemu celowi niż wymiana danych.**

Wskazują na to cechy pakietów uTP – okrągłe wartości timestampów, nieprzestrzeganie protokołu uTP, ignorowanie wiadomości ICMP o zamkniętym porcie UDP. Wybieranie adresów docelowych z honeynetów systemu ARAKIS przemawia za tą hipotezą.

Cele anomalii

Najbardziej prawdopodobne cele obserwowanej anomalii, to:

- **Transmisje służą zatruwaniu sieci uTP/BT**

Z danych zebranych z publicznych trackerów wynika, że stosunek seederów do leecherów dzielących się plikami o hashu 057a315b89b54e53e2ee583dd5cd9ef60648805e i innych hashach dot. filmu „Avgust. Vosmogo" jest niespotykany i może być wynikiem zatruwania elementów sieci uTP/BT (np. przez dystrybuowanie fałszywych danych dot. peerów – ciągów zer).

- **Transmisje służą mapowaniu sieci uTP/BT**

Możliwe, że transmisje służą do wyznaczenia mapy sieci węzłów sieci uTP/BT. Automat mapujący klasyfikowałby badany węzeł jako klienta uTP na podstawie odpowiedzi:

- Poprawna odpowiedź uTP – węzeł jest klientem uTP,
- Zła odpowiedź uTP – węzeł nie jest klientem uTP.

Przeciwko tej hipotezie jednak świadczą następujące fakty:

- Pomimo odpowiedzi ICMP Port unreachable źródło wysyła kolejny pakiet, chociaż klasyfikacji można dokonać na podstawie pierwszej odpowiedzi,
- Część pakietów posiada sfałszowany adres źródłowy, co praktycznie uniemożliwia automatowi odebranie odpowiedzi i dokonanie klasyfikacji.

- **Transmisje stanowią atak na systemy teleinformatyczne**

Możliwe, że wysyłane pakiety wprowadzają niektóre aplikacje w nieprzewidziany przez ich autora stan – są exploitami. Z pobieżnej analizy publicznie dostępnych informacji dot. podatności klienta uTorrent nie wynika, że ta hipoteza jest prawdziwa, jednak posiadamy za mało wiedzy na temat innych klientów oraz nieopublikowanych luk, żeby stwierdzić to z pewnością. Możliwe, że niektóre cechy pakietów uTP (np. zerowa wartość numeru potwierdzenia) lub BT (zera w polu peer id) mogą wprowadzić niektóre aplikacje w nieprzewidziany stan.

Anomalia poprzez swój charakter (duża część ruchu z całego dnia) stanowi wyraźne zakłócenie pracy systemu teleinformatycznego, czego dobrym dowodem jest generowanie dużej ilości fałszywych alarmów wysokiego poziomu. W kontekście polskiego prawa, europejskiej konwencji o cyberprzestępczości i kodeksów amerykańskich (oraz pewnie wielu innych źródeł prawa w różnych krajach) można dyskutować, czy tworzenie tego ruchu jest zgodne z prawem.

- **Obserwowany przez nas ruch przynajmniej częściowo jest echem**

Możliwe, że część zarejestrowanych przez nas pakietów jest echem zdarzeń (incydentów), które wystąpiły w innych sieciach.

Znaczenie anomalii

Oto najbardziej prawdopodobne znaczenie obserwowanej anomalii:

- **Zatruwanie sieci / mapowanie**

Za tą tezą przemawiają dane pobrane z publicznych trackerów. Bez wnikania w szczegóły reakcji klientów torrentowych można stwierdzić, że w trackerach rejestruje się mało peerów pobierających dyskutowane zasoby. Możliwe, że jest to wynik funkcjonowania mechanizmów, które wywołują opisywaną anomalię. Można bez problemu wskazać przynajmniej jedną grupę potencjalnych autorów i beneficjentów zatruwania sieci uTP: koncerny multimedialne lub ich podwykonawcy. Prowadzenie przez te instytucje tego typu kampanii nie byłoby precedensem. Niewykluczone też, że generowany ruch ma służyć mapowaniu sieci BitTorrent i zbieraniu informacji, które zostaną wykorzystane w innych projektach.

- **Błędna implementacja / eksperyment**

Nieprzestrzeganie protokołu uTP może być wynikiem błędnej implementacji protokołu uTP w mało popularnym lub niedojrzałym kliencie BitTorrentowym. Niewykluczone też, że omawiana anomalia jest wynikiem jakiegoś sieciowego eksperymentu.

- **Ruch maskujący**

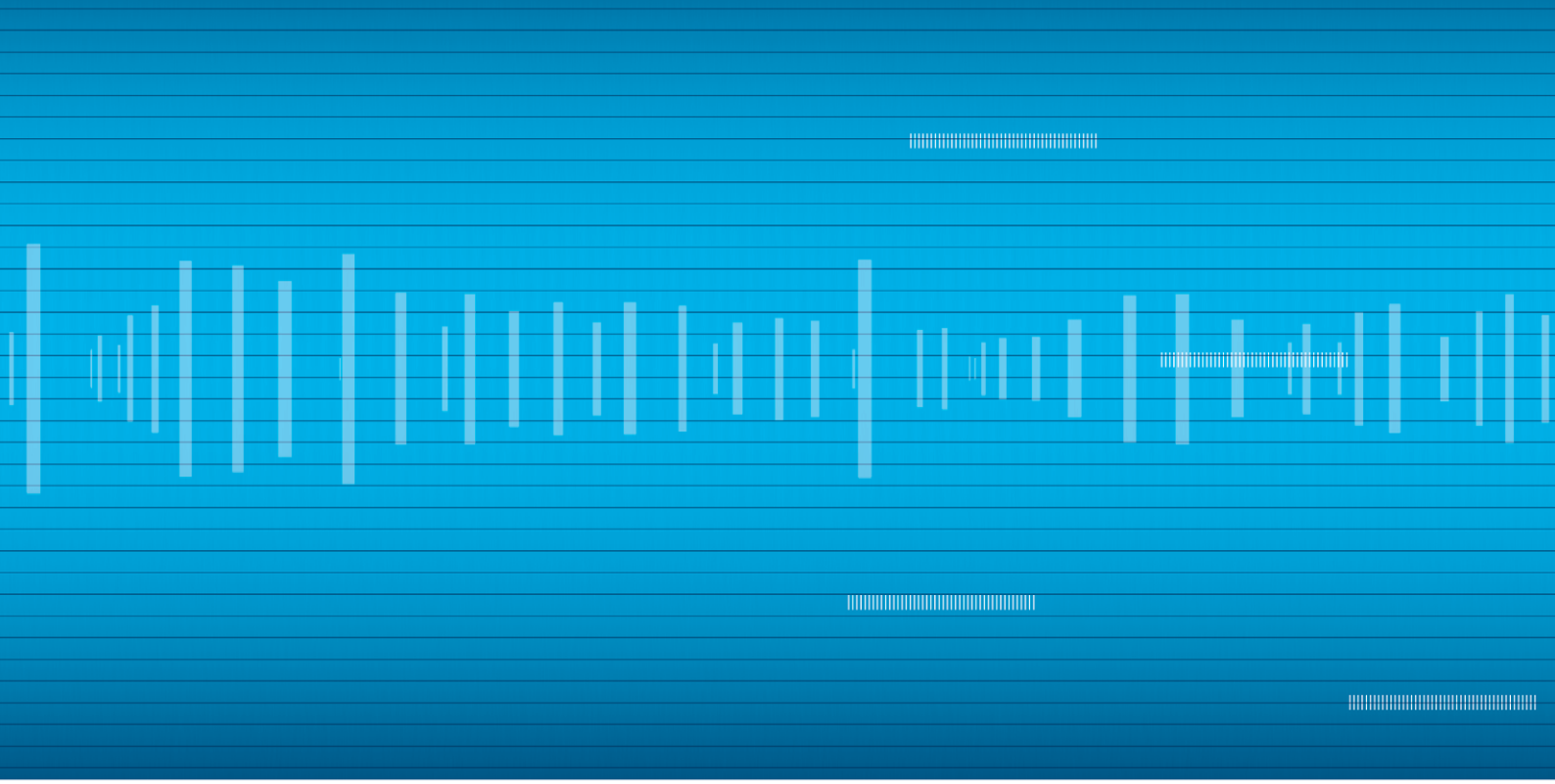
Jeśli uznać, że ruch składający się na anomalię zawiera mieszankę prawdziwych i fałszywych źródeł, można wysunąć przypuszczenie, że część tego ruchu posiada dobrze określone przyczyny i skutki, natomiast część (większość) stanowi ruch maskujący. Ruch zawierający poprawne numery sekwencji i adresy (niepowodujący zerwania sesji), pomimo że w mniejszej ilości, mógłby okazać się efektywny przy zatruwaniu lub mapowaniu sieci uTP.

- **Echo ataków na inne sieci**

Możliwe, że część obserwowanego przez nas w honeynecie ruchu stanowi echo ataku prowadzonego w innych sieciach. Części ruchu, które czynią tą możliwość bardziej prawdopodobną to m.in.: pakiety z flagami uTP STATE (odpowiednik pakietów TCP SYN/ACK przy echach ataków DDoS) oraz transmisje połączeniowe z identyfikatorami peerów, które wyglądają na poprawne.

6.3.5 Podsumowanie

Po dotychczasowej analizie opisywanego ruchu nie udało się ustalić jednoznacznie jego źródła ani przeznaczenia. Rejestrowane pakiety są na tyle skomplikowane, że można z dużym przypuszczeniem stwierdzić, iż zostały specjalnie zaprojektowane. Wątpliwą kwestią jest jedynie, czy ich postać i ilość jest wynikiem celowego działania (np. zatruwanie sieci), czy też błędem w oprogramowaniu.



Kontakt

Zgłaszanie incydentów:	cert@cert.pl
Zgłaszanie spamu:	spam@cert.pl
Informacja:	info@cert.pl
Klucz PGP:	http://www.trusted-introducer.nl/teams/0x553FEB09.asc
Strona WWW:	http://www.cert.pl/
	http://facebook.com/CERT.Polska
RSS Feed:	http://www.cert.pl/rss
Twitter:	@CERT_Polska
	@CERT_Polska_en
Adres:	NASK / CERT Polska
	ul. Wąwozowa 18
	02-796 Warszawa
tel.:	+48 22 3808 274
fax:	+48 22 3808 399